Trustworthy Computing,
Academic Advisory Board - July '05

Internet Explorer 7: Secure By Design and Default

Rob Franco, Lead Program Manager
Internet Explorer

About this presentation

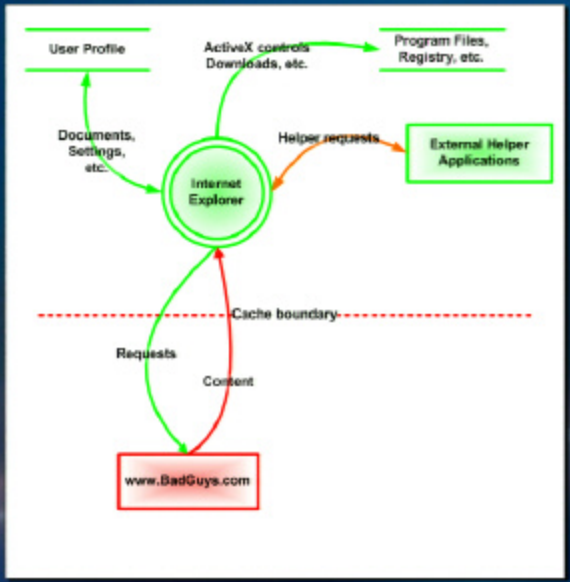
- Overview
- In this presentation, we will cover:
  - Guiding principles
  - High level browser threat model
    - Data flow and Architecture of IE
    - Threats for UI, Network request and Page Rendering layers
  - How IE7 addresses the threats
    - Phishing-filter mitigation
    - Window restrictions update
    - Safer UI for security decisions and browser settings
    - Unified URL parsing architecture
    - Cross Domain Architecture Updates
    - ActiveX mitigations
    - Buffer overruns mitigations
    - Low-rights IE mitigation on Vista

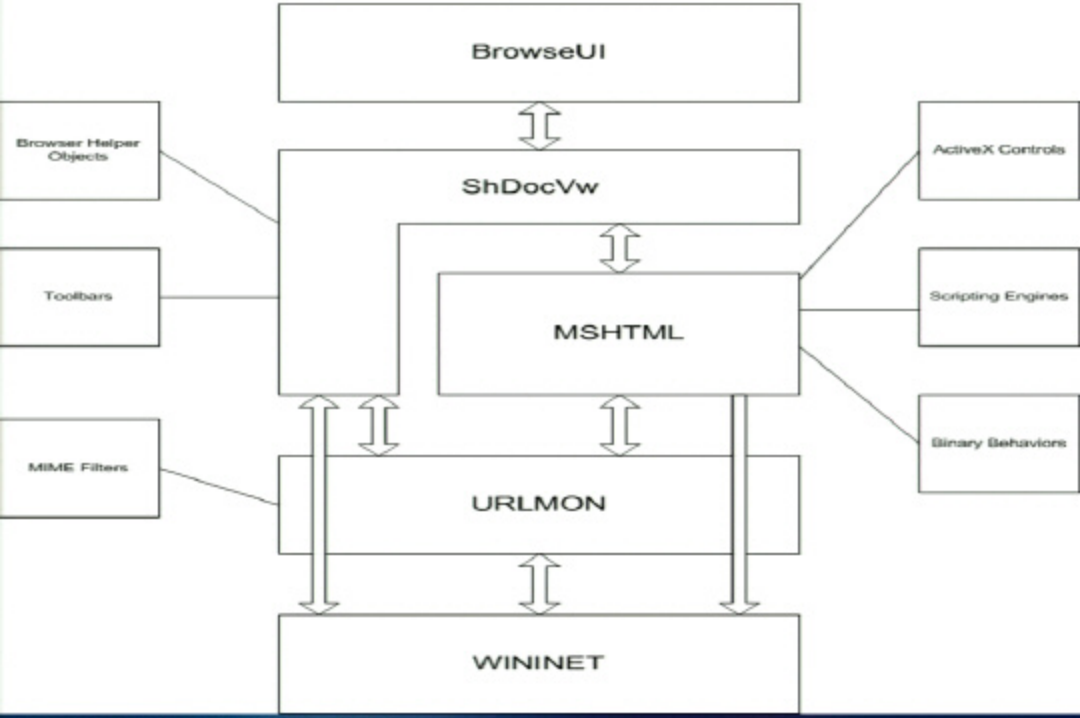
Guiding principles

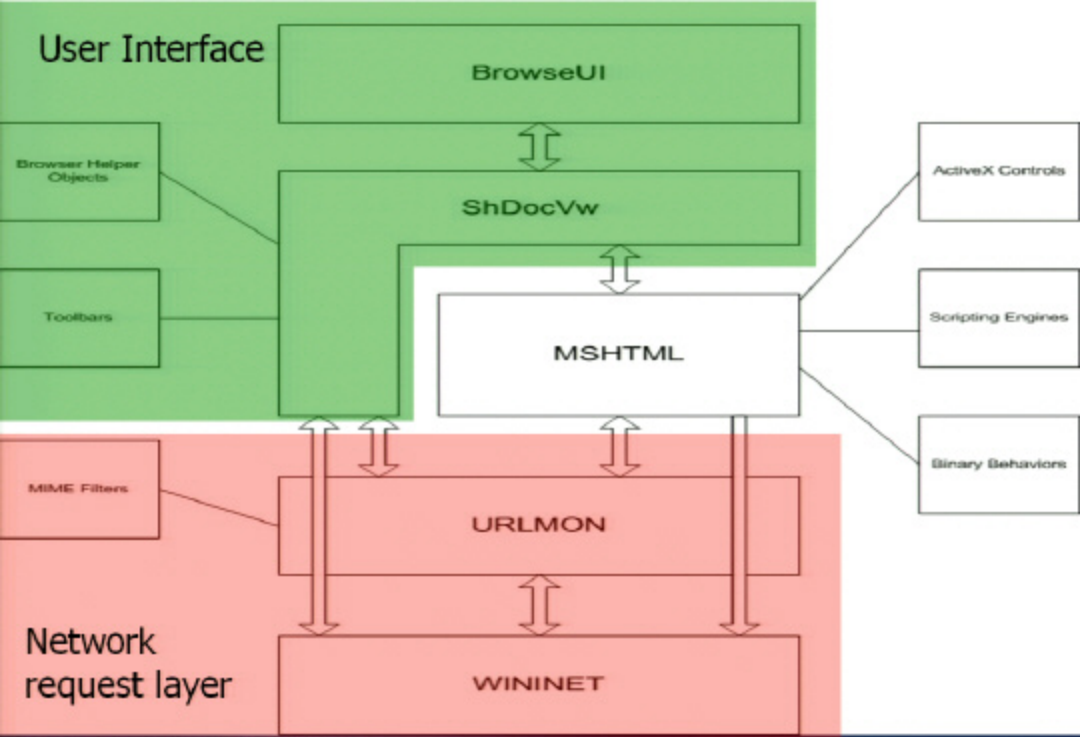
- Balance our customers' need for browsing that's powerful but also secure
  - Architectural changes eradicate classes of vulns
  - Mitigations reduce severity or prevent future vulns
  - Security Updates address targeted issues and variations
- Every release goes through threat modeling, penetration testing and code analysis tools

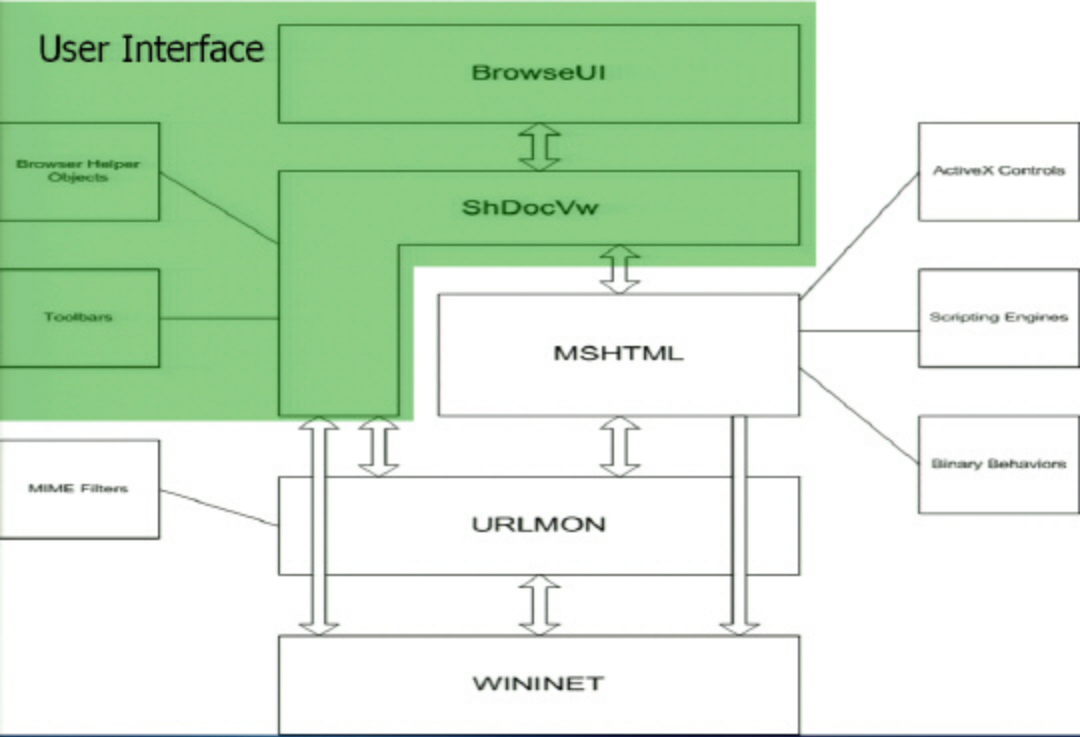
Browser security
Data flow

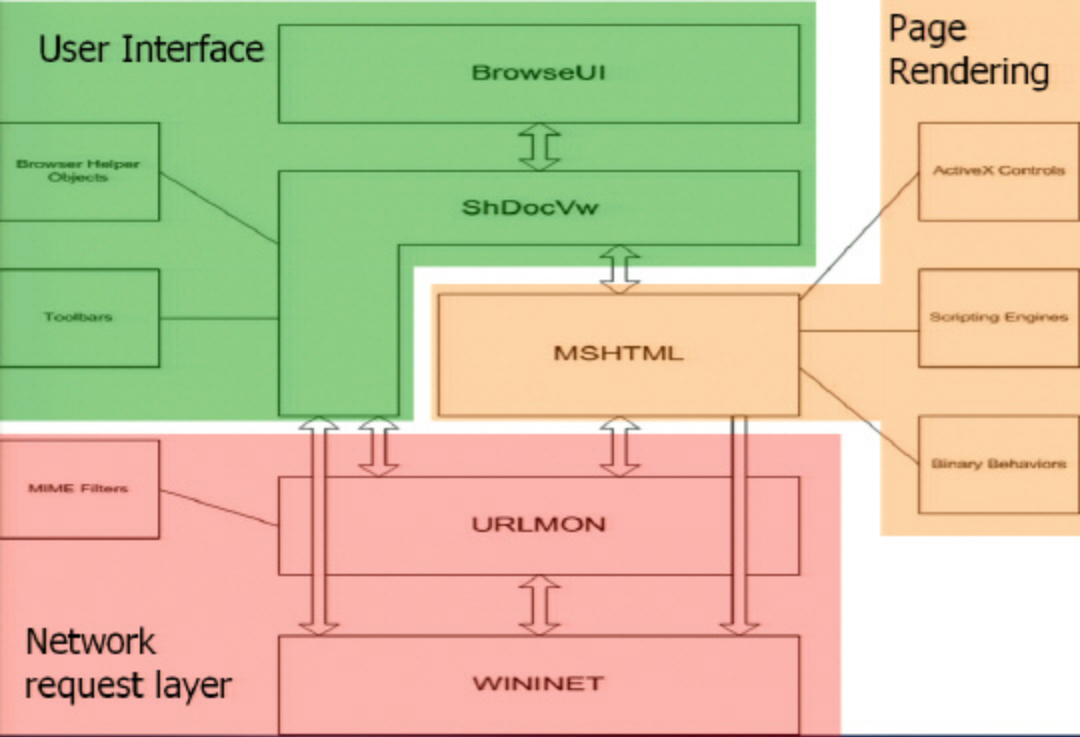
- Outbound:
  - URLs
  - HTTP requests
  - Auth and cookie data
- Inbound:
  - URLs
  - HTML
  - Script
  - Non-IE files




BrowseUI
Browser Helper Objects
ShDocVw
ActiveX Controls
Toolbars
MSHTML
Scripting Engines
Binary Behaviors
MIME Filters
URLMON
WININET


User Interface
BrowseUI
Browser Helper Objects
ShDocVw
ActiveX Controls
Toolbars
MSHTML
Scripting Engines
Binary Behaviors
MIME Filters
URLMON
Network request layer
WININET


User Interface
BrowseUI
Browser Helper Objects
ShDocVw
Toolbars
ActiveX Controls
MSHTML
Scripting Engines
Binary Behaviors
MIME Filters
URLMON
WININET

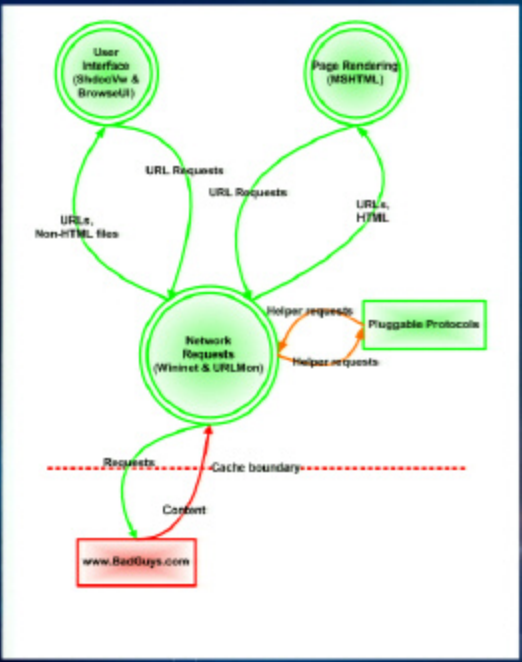

User Interface
BrowseUI
Browser Helper Objects
ShDocVw
Toolbars
Page Rendering
ActiveX Controls
MSHTML
Scripting Engines
Binary Behaviors
MIME Filters
URLMON
Network request layer
WININET

Threats in User Interface

Sample Threats:

- URLs parsed incorrectly
  - Domain spoofed
  - buffer overrun
  - User can't read URL
- Dangerous files launch & install
  - User clicks "OK"
  - Logic error in prompt
- Scripted Windows trick user
  - Overlays UI warnings
- User lowers security settings

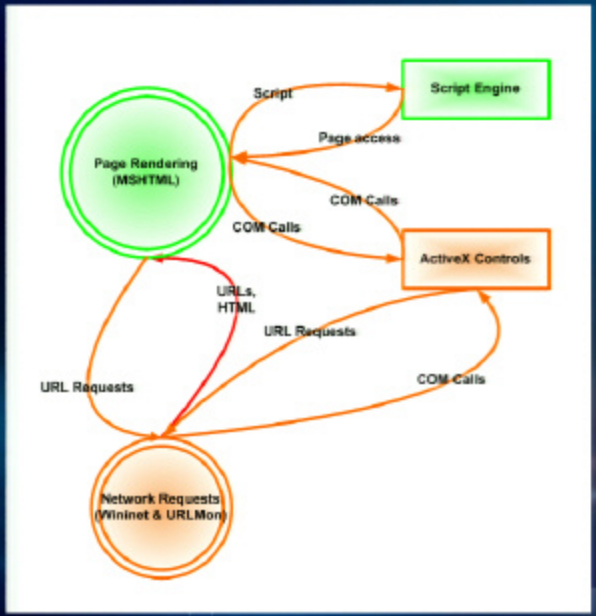
Threats in Network Request Layer



Sample Threats:

- Auth Credentials encryption cracked
- URL parsed incorrecty
  - buffer overrun
  - Security settings not enforced
- Data sniffer buffer overrun or logic failure
- Faulty pluggable protocol loads

Threats in Page Rendering



Sample Threats

- URLs parsed incorrectly
  - buffer overrun
  - Page Access rules fail
- HTML parser buffer overrun
- Faulty COM object loads
- Page Access rules fail
  - Unsafe access defaults
  - Page Redirects

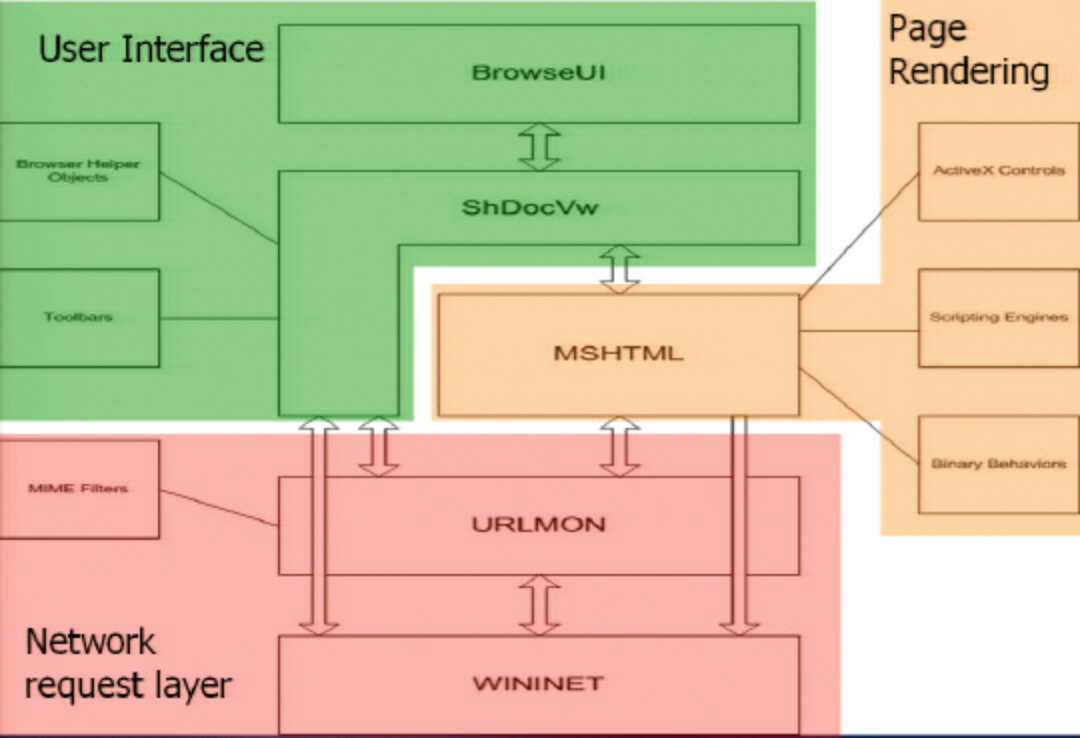
About this presentation

- Overview
- In this presentation, we will cover:
  - Guiding principles
  - High level browser threat model
    - Data flow and Architecture of IE
    - Threats for UI, Network request and Page Rendering layers
  - How IE7 addresses the threats
    - Phishing-filter mitigation
    - Window restrictions update
    - Safer UI for security decisions and browser settings
    - Unified URL parsing architecture
    - **Cross Domain Architecture Updates**
    - ActiveX mitigations
    - Buffer overruns mitigations
    - Low-rights IE mitigation on Vista

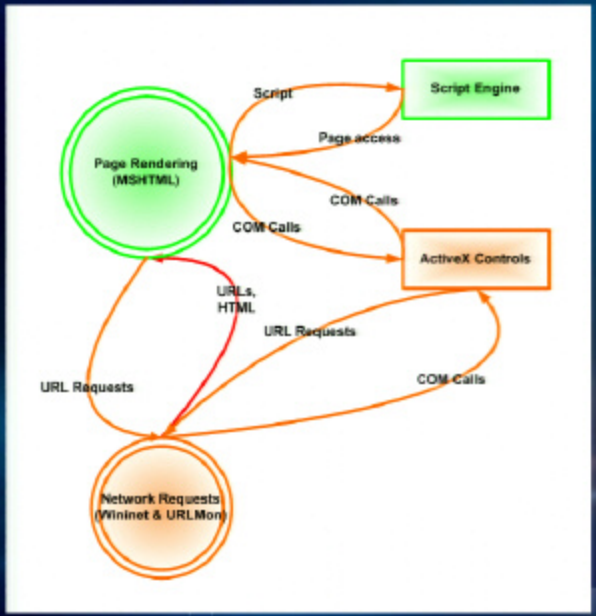
Threats in User Interface

Sample Threats:

- URLs parsed incorrectly
  - Domain spoofed
  - buffer overrun
  - User can't read URL
- Dangerous files launch & install
  - User clicks "OK"
  - Logic error in prompt
- Scripted Windows trick user
  - Overlays UI warnings
- User lowers security settings


User Interface
BrowseUI
Browser Helper Objects
ShDocVw
Toolbars
Page Rendering
ActiveX Controls
MSHTML
Scripting Engines
Binary Behaviors
MIME Filters
URLMON
Network request layer
WININET

Threats in Page Rendering



Sample Threats

- URLs parsed incorrectly
  - buffer overrun
  - Page Access rules fail
- HTML parser buffer overrun
- Faulty COM object loads
- Page Access rules fail
  - Unsafe access defaults
  - Page Redirects

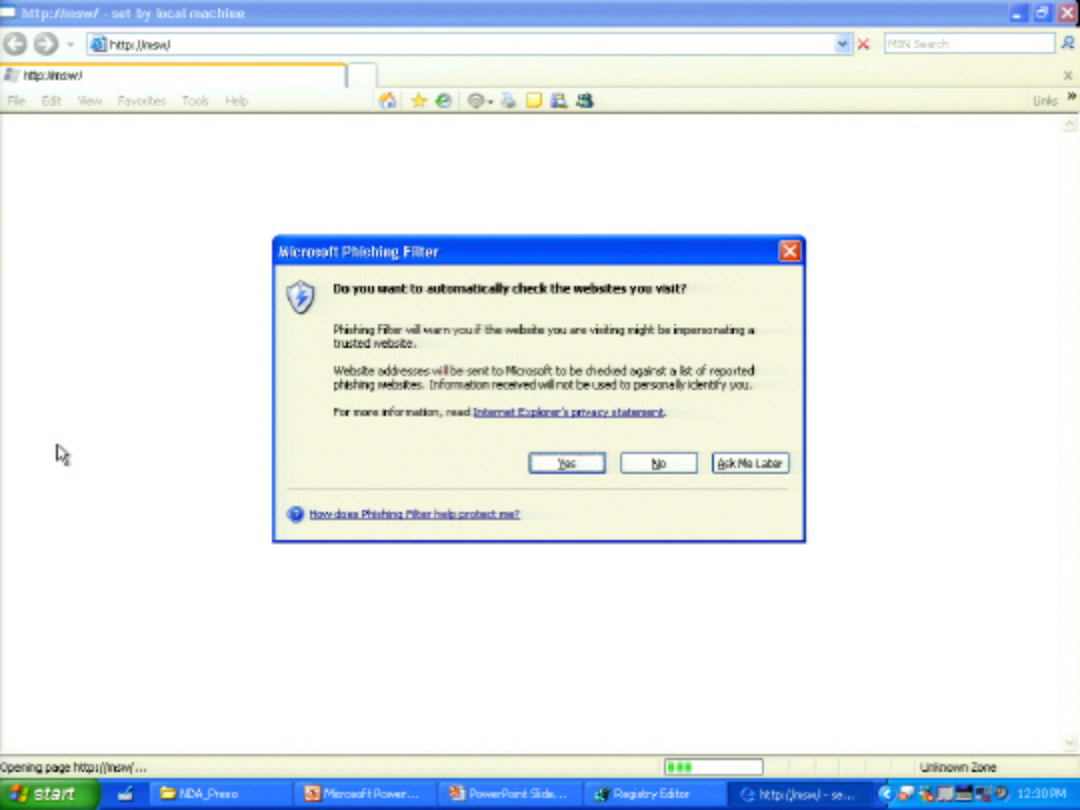
About this presentation

- Overview
- In this presentation, we will cover:
  - Guiding principles
  - High level browser threat model
    - Data flow and Architecture of IE
    - Threats for UI, Network request and Page Rendering layers
  - How IE7 addresses the threats
    - Phishing-filter mitigation
    - Window restrictions update
    - Safer UI for security decisions and browser settings
    - Unified URL parsing architecture
    - **Cross Domain Architecture Updates**
    - ActiveX mitigations
    - Buffer overruns mitigations
    - Low-rights IE mitigation on Vista

Demonstration: Spoof-proof

In this demonstration, you will learn how Internet Explorer 7:

- Uses a dynamic Phishing-Filter to protect users from phishing sites
- Uses heuristics to detect suspicious sites
- Highlights the user experience for secure sites (SSL)


http://nsw/ - set by local machine
http://nsw/
MSN Search
http://nsw/
File Edit View Favorites Tools Help
Links
Microsoft Phishing Filter
Do you want to automatically check the websites you visit?
Phishing Filter will warn you if the website you are visiting might be impersonating a trusted website.
Website addresses will be sent to Microsoft to be checked against a list of reported phishing websites. Information received will not be used to personally identify you.
For more information, read Internet Explorer's privacy statement.
Yes
No
Ask Me Later
How does Phishing Filter help protect me?
Opening page http://nsw/...
Unknown Zone
start
NDA_Press
Microsoft Power...
PowerPoint Slide...
Registry Editor
http://nsw/ - se...
12:10 PM

Microsoft Web-MSWeb - set by local machine

http://insweb/default.aspx

MSN Search

Microsoft Web-MSWeb

File Edit View Favorites Tools Help

Links

microsoftweb

UPDATED: THURSDAY, JULY 28, 2005

My Site Help

Microsoft

Top Tasks: I Need to Find... Search: Advanced Search Search Tips

News
- Industry News
- World News
- News Archive

Look It Up
- Directory
- Library
- Org Browser

Corporate Services
- Campus
- Travel
- Workplace Services
- Purchasing
- Vendors

About Microsoft
- Company Overview
- History & Culture
- What's Shipping

Core Businesses
- Business Solutions
- Home & Entertainment

Security Alert: eTrust Required by Aug. 15

All work systems connected to the Microsoft corporate network are required to run Microsoft's site-licensed antivirus software, eTrust. Beginning Aug. 15, any system found not to be running eTrust will be disconnected from the network.

Allchin: A Window Into Vista

Q&A: Jim Allchin, group vice president managing all Windows development work, discusses the beta release of Vista, its features and limitations, and hurdles remaining before the software's eventual launch.

OTHER TOP STORIES

- Bellmer: Our Achievements And Growth In FY05
- Empowering People With Disabilities
- Reminder: Company Picnic Is This Weekend

Subscribe to News Alerts

BREAKFAST SERIES

The Word From Wall Street

Coming Tomorrow! Top market analysts will share their thoughts about Microsoft, the software industry and broader market trends in an informal one-hour session.

Breakfast Series

CALENDAR OF EVENTS

7/28/2005	A Conversation with Microsoft's CIO Ron Markezich: Employee Productivity
7/29/2005	Breakfast Series: The Word from Wall Street
7/30/2005	Microsoft Company Picnic
7/31/2005	Microsoft Night With The Seattle Storm!
8/1/2005	TechReady1 - Live Meetings Available

See more events

Glossary Lookup

Enter acronym or term

DIRECTORY

Key Sites
Classifieds, eCompany Store, HRWeb, ITWeb, Micronews, Microsoft.com, MS Dining, Library, MSN, MSNBC

CAMPUS
- Food
- Maps & Building Services
- Meeting Rooms

more...

HR & BENEFITS
- Benefits
- Giving
- Human Resources

more...

PRODUCT DEVELOPMENT
- Brand
- Bugs
- Dev Tools

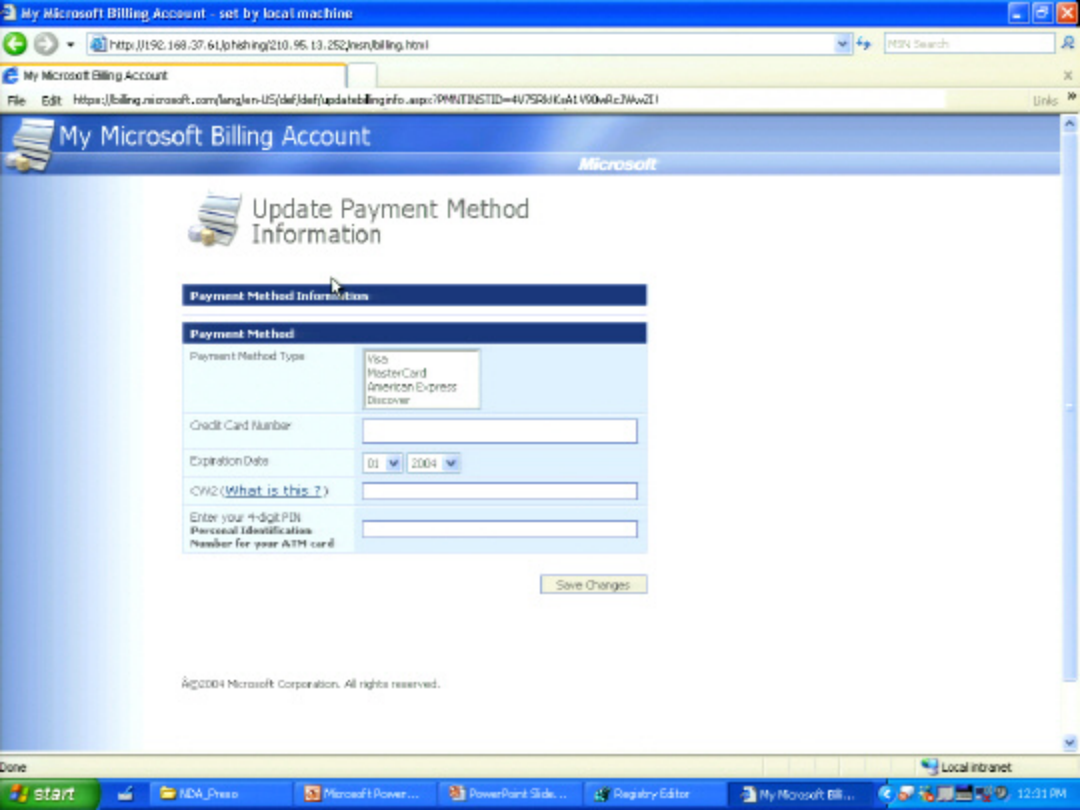
more...

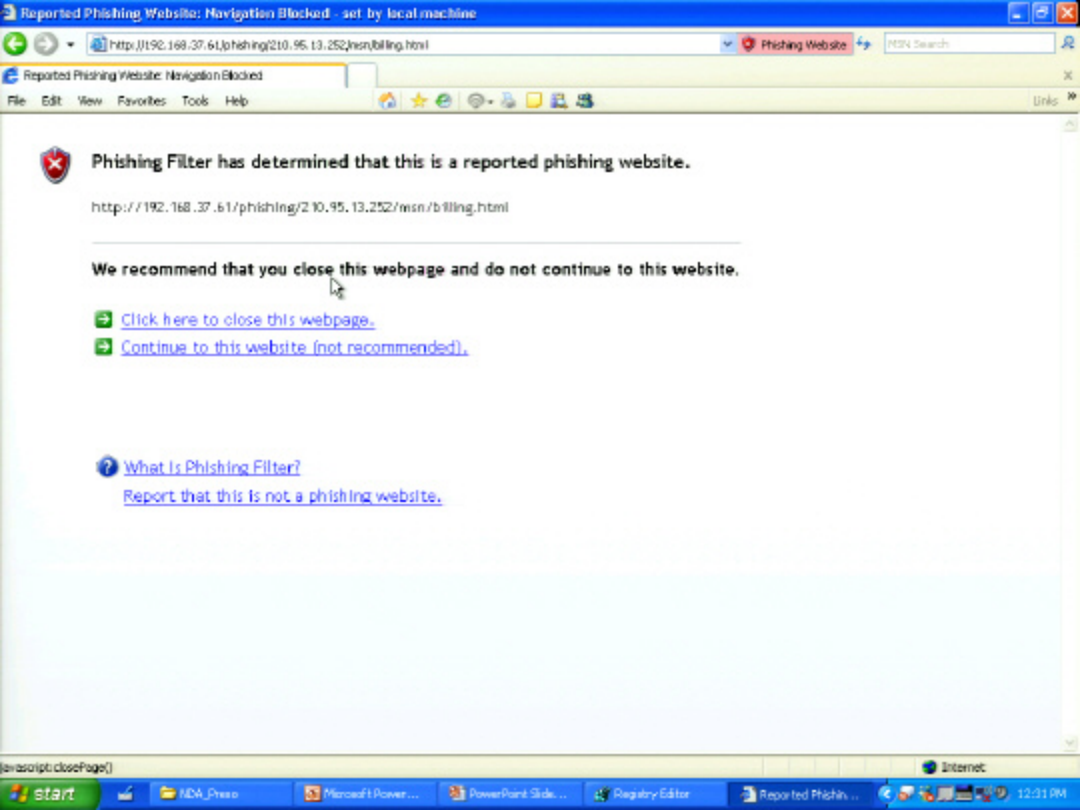
PRODUCTS & TECHNOLOGIES

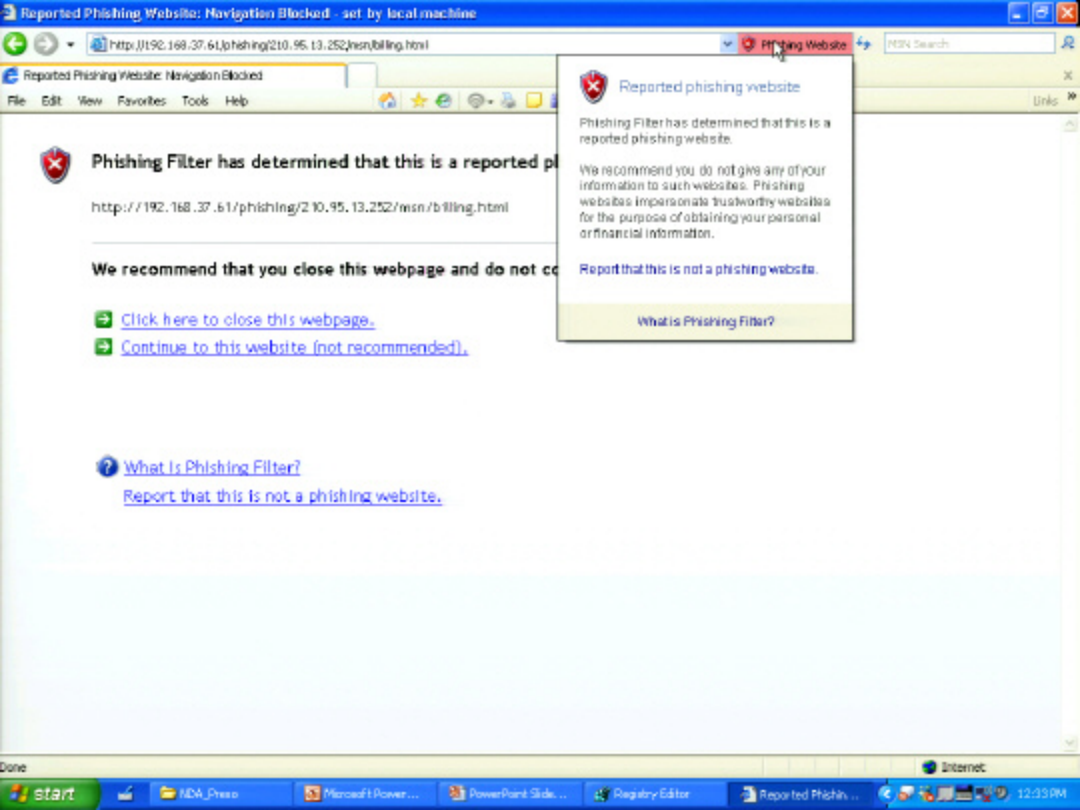
Opening page http://192.168.37.61/phishing/210.95.13.252/msn/billing.html...

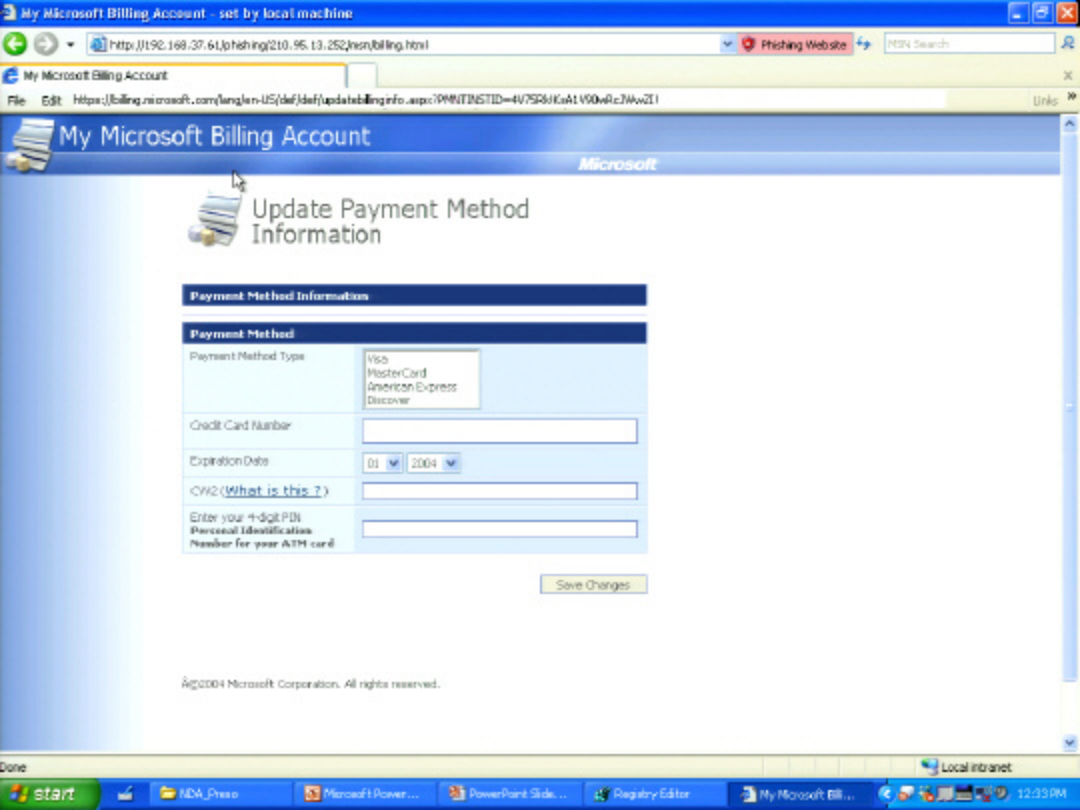
Local intranet

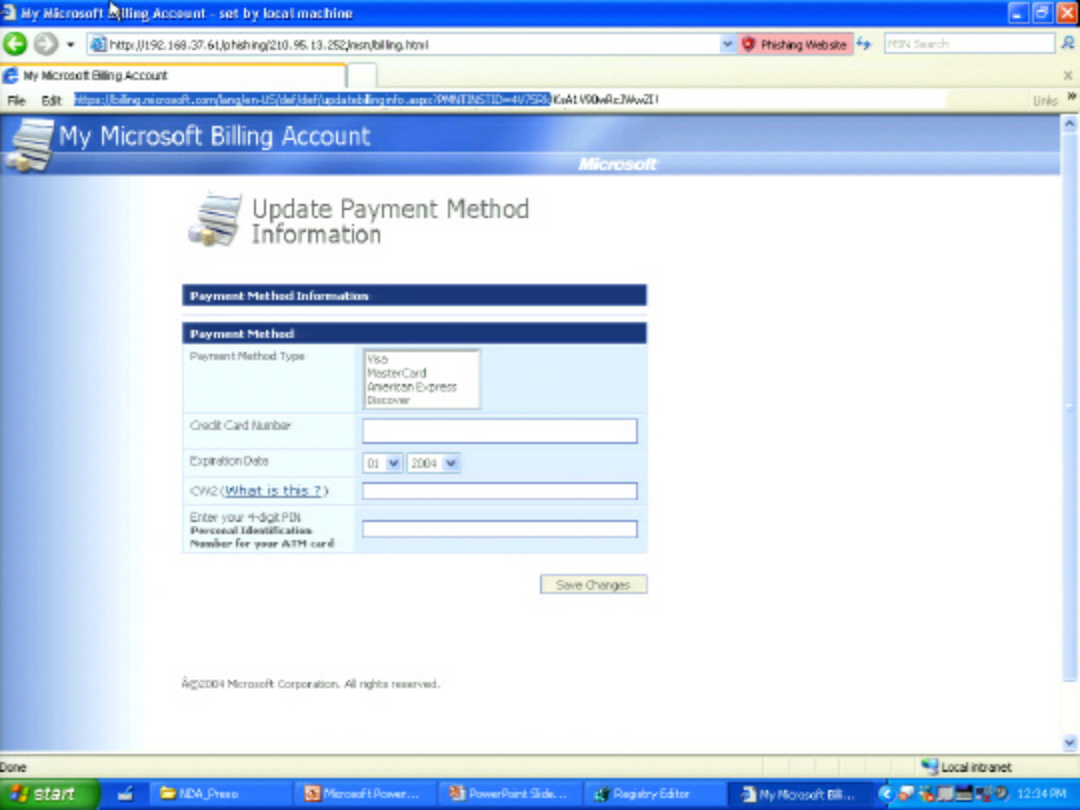
start MDA_Press Microsoft Power... PowerPoint Slide... Registry Editor Microsoft Web-M... 12:31 PM

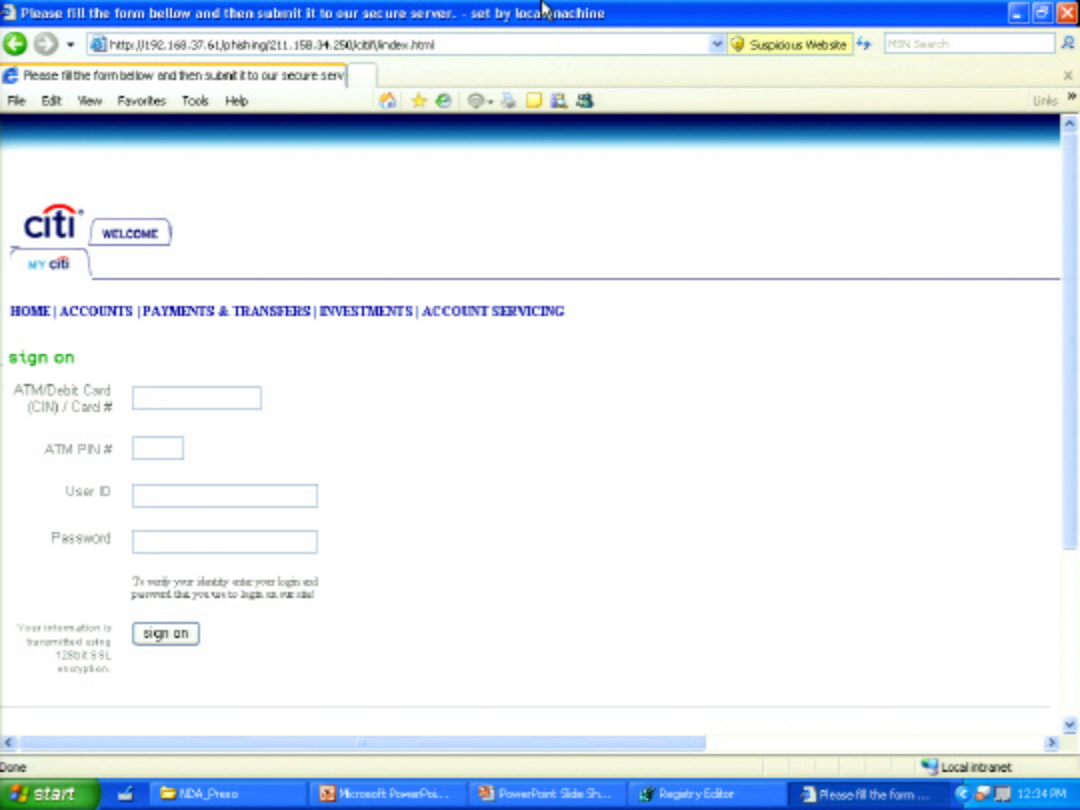

My Microsoft Billing Account - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
My Microsoft Billing Account
File Edit https://billing.microsoft.com/lang/en-US/def/def/updatebillinginfo.aspx?PMNTINSTID=4V7SR6KsAtV90wRcJWwZI
My Microsoft Billing Account
Microsoft
Update Payment Method Information
Payment Method Information
Payment Method
Payment Method Type
Visa
MasterCard
American Express
Discover
Credit Card Number
Expiration Date
01
2004
CVV2 (What is this ?)
Enter your 4-digit PIN
Personal Identification Number for your ATM card
Save Changes
©2004 Microsoft Corporation. All rights reserved.
Done
Local intranet
start
MDA_Press
Microsoft Power...
PowerPoint Slide...
Registry Editor
My Microsoft Bill...
12:31 PM

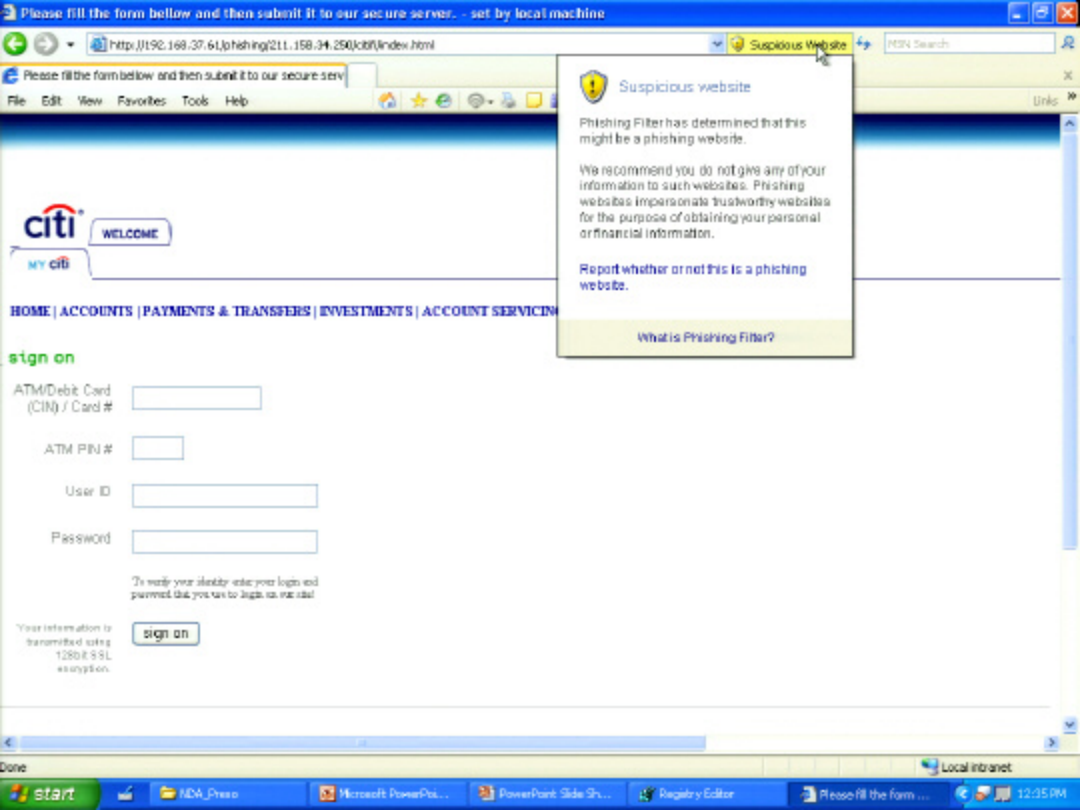

Reported Phishing Website: Navigation Blocked - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
Phishing Website
Reported Phishing Website: Navigation Blocked
File Edit View Favorites Tools Help
Phishing Filter has determined that this is a reported phishing website.
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
What is Phishing Filter?
Report that this is not a phishing website.
javascript:closePage()
Internet
start
MDA_Presa
Microsoft Power...
PowerPoint Slide...
Registry Editor
Reported Phishin...
12:31 PM

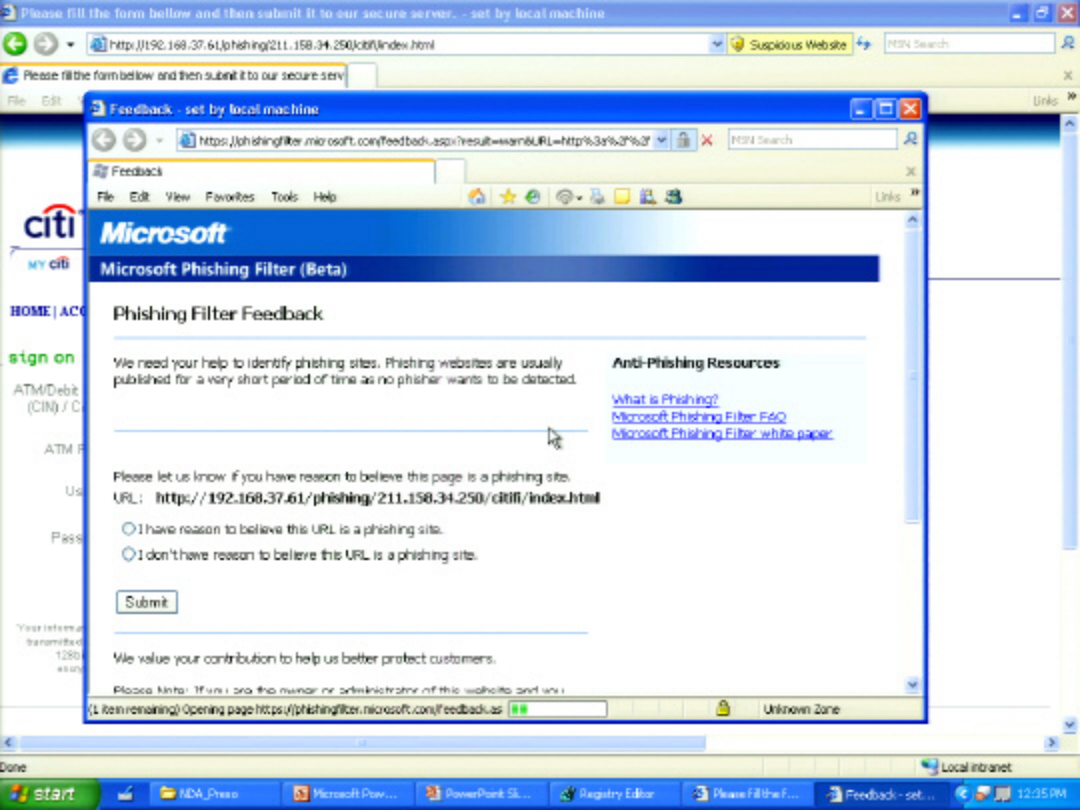

Reported Phishing Website: Navigation Blocked - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
Phishing Website
MSN Search
Reported Phishing Website: Navigation Blocked
File Edit View Favorites Tools Help
Links
Reported phishing website
Phishing Filter has determined that this is a reported phishing website.
We recommend you do not give any of your information to such websites. Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.
Report that this is not a phishing website.
What is Phishing Filter?
Phishing Filter has determined that this is a reported ph
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
We recommend that you close this webpage and do not co
Click here to close this webpage.
Continue to this website (not recommended).
What is Phishing Filter?
Report that this is not a phishing website.
Done
Internet
start
MDA_Presc
Microsoft Power...
PowerPoint Slide...
Registry Editor
Reported Phishin...
12:13 PM

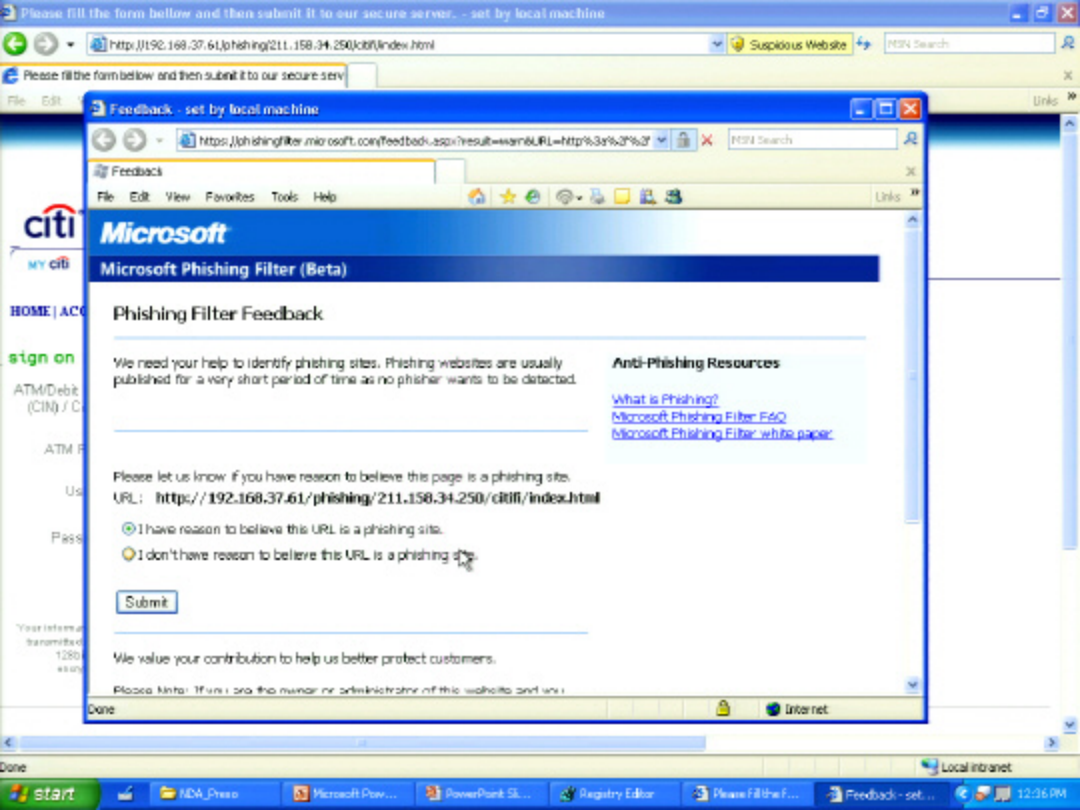

My Microsoft Billing Account - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
Phishing Website
My Microsoft Billing Account
File Edit https://billing.microsoft.com/lang/en-US/def/def/updatebillinginfo.aspx?PMNTINSTID=4V7SR6KGAtV00vRcJWvvZI
My Microsoft Billing Account
Microsoft
Update Payment Method Information
Payment Method Information
Payment Method
Payment Method Type
Visa
MasterCard
American Express
Discover
Credit Card Number
Expiration Date
01
2004
CW2 (What is this ?)
Enter your 4-digit PIN Personal Identification Number for your ATM card
Save Changes
©2004 Microsoft Corporation. All rights reserved.
Done
Local intranet
start
MDA_Presa
Microsoft Power...
PowerPoint Slide...
Registry Editor
My Microsoft Bill...
12:13 PM

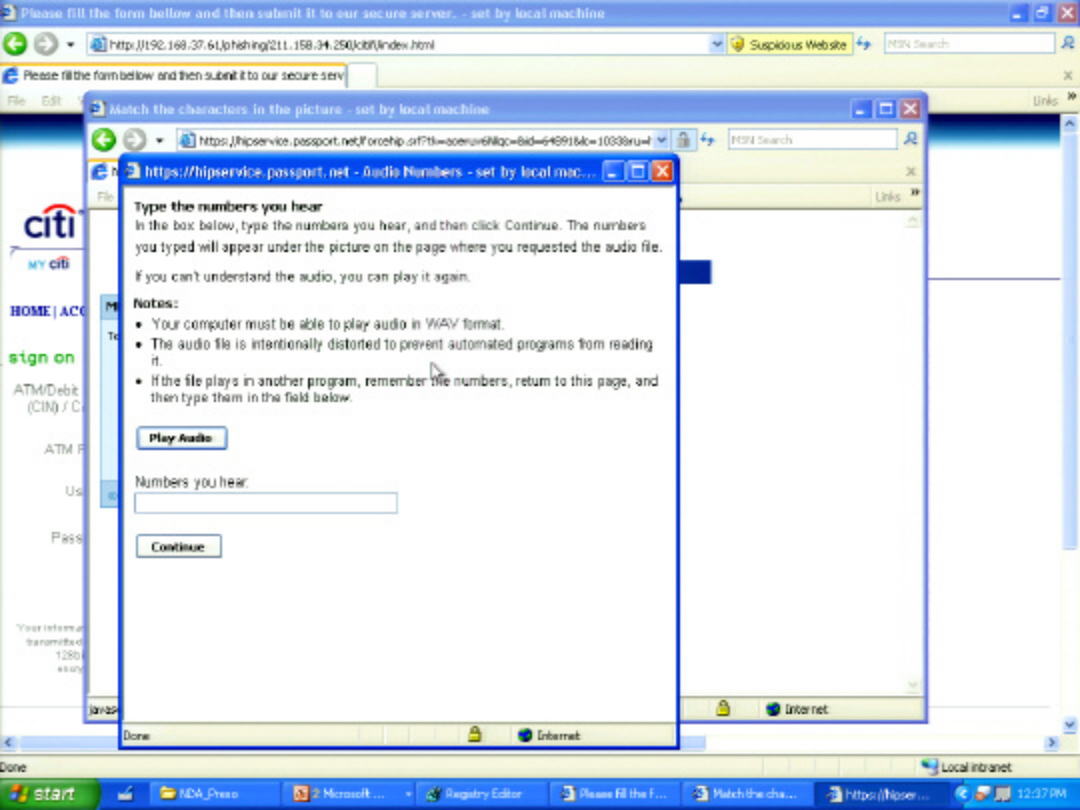

My Microsoft Billing Account - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
Phishing Website
My Microsoft Billing Account
File Edit
https://Billing.microsoft.com/lang/en-US/def/def/updatebillinginfo.aspx?PMNTINSTID=4V7SR
My Microsoft Billing Account
Microsoft
Update Payment Method Information
Payment Method Information
Payment Method
Payment Method Type
Visa
MasterCard
American Express
Discover
Credit Card Number
Expiration Date
01
2004
CVV2 (What is this ?)
Enter your 4-digit PIN
Personal Identification Number for your ATM card
Save Changes
©2004 Microsoft Corporation. All rights reserved.
Done
Local intranet
start
MDA_Press
Microsoft Power...
PowerPoint Slide...
Registry Editor
My Microsoft Bill...
12:14 PM

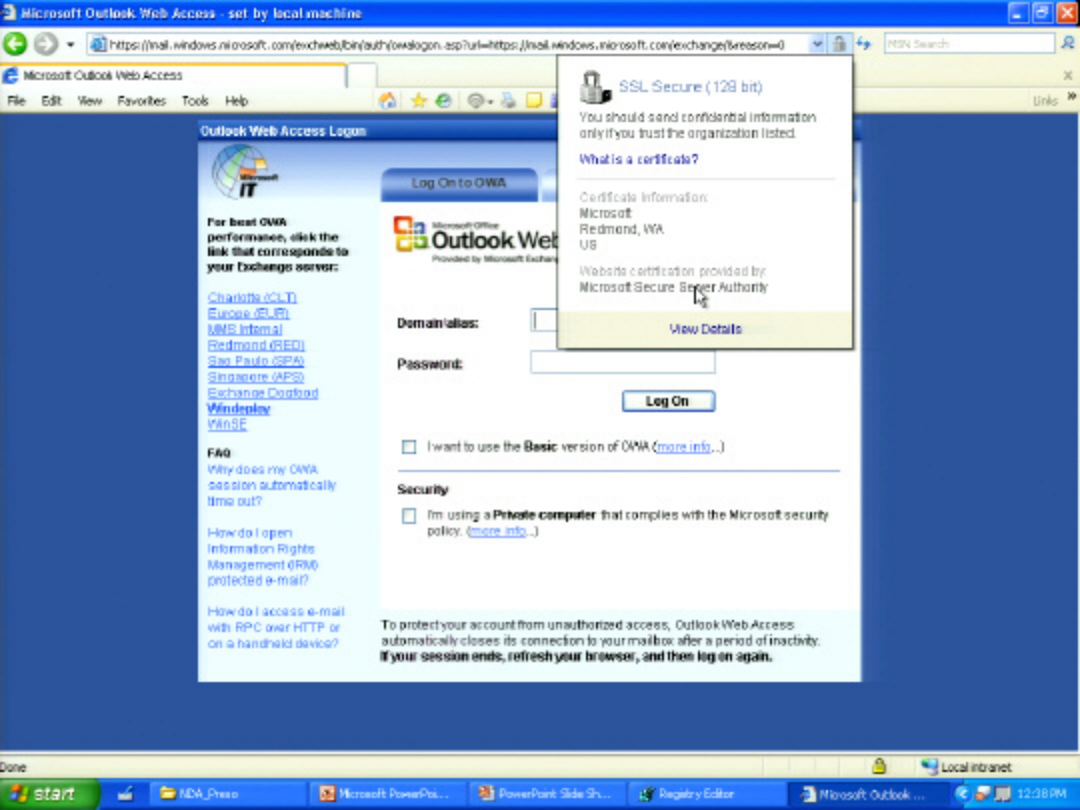

Please fill the form bellow and then submit it to our secure server. - set by local machine
http://192.168.37.61/phishing/211.158.34.250/citi/index.html
Suspicious Website
Please fill the form bellow and then submit it to our secure serv
File Edit View Favorites Tools Help
citi
WELCOME
MY citi
HOME | ACCOUNTS | PAYMENTS & TRANSFERS | INVESTMENTS | ACCOUNT SERVICING
sign on
ATM/Debit Card (CIN) / Card #
ATM PIN #
User ID
Password
To verify your identity enter your login and password that you use to login on our site!
Your information is transmitted using 128bit SSL encryption.
sign on
Done
Local intranet
start
MDA_Presc
Microsoft PowerPoi...
PowerPoint Slide Sh...
Registry Editor
Please fill the form ...
12:34 PM


Please fill the form bellow and then submit it to our secure server. - set by local machine
http://192.168.37.61/phishing/211.158.34.250/citi/index.html
Suspicious Website
Please fill the form bellow and then submit it to our secure serv
File Edit View Favorites Tools Help
Suspicious website
Phishing Filter has determined that this might be a phishing website.
We recommend you do not give any of your information to such websites. Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.
Report whether or not this is a phishing website.
What is Phishing Filter?
citi
WELCOME
MY citi
HOME | ACCOUNTS | PAYMENTS & TRANSFERS | INVESTMENTS | ACCOUNT SERVICING
sign on
ATM/Debit Card (CIN) / Card #
ATM PIN #
User ID
Password
To verify your identity, enter your login and password that you use to login on our site.
Your information is transmitted using 128bit SSL encryption.
sign on
Done
Local intranet
start
MDA_Press
Microsoft PowerPoi...
PowerPoint Slide Sh...
Registry Editor
Please fill the form ...
12:15 PM


Please fill the form bellow and then submit it to our secure server. - set by local machine
http://192.168.37.61/phishing/211.158.34.250/citifi/index.html
Suspicious Website
Please fill the form bellow and then submit it to our secure serv
Feedback - set by local machine
https://phishingfilter.microsoft.com/feedback.aspx?result=warn&URL=http%3a%2f%2f
Feedback
File Edit View Favorites Tools Help
Microsoft
Microsoft Phishing Filter (Beta)
Phishing Filter Feedback
We need your help to identify phishing sites. Phishing websites are usually published for a very short period of time as no phisher wants to be detected.
Anti-Phishing Resources
What is Phishing?
Microsoft Phishing Filter FAQ
Microsoft Phishing Filter white paper
Please let us know if you have reason to believe this page is a phishing site.
URL: http://192.168.37.61/phishing/211.158.34.250/citifi/index.html
I have reason to believe this URL is a phishing site.
I don't have reason to believe this URL is a phishing site.
Submit
We value your contribution to help us better protect customers.
Please Note: If you are the owner or administrator of this website and you
(1 item remaining) Opening page https://phishingfilter.microsoft.com/feedback.as
Unknown Zone
Done
Local intranet
start
MDA_Press
Microsoft Pow...
PowerPoint Sl...
Registry Editor
Please Fill the F...
Feedback - set...
12:15 PM


Please fill the form bellow and then submit it to our secure server. - set by local machine
http://192.168.37.61/phishing/211.158.34.250/citifi/index.html
Suspicious Website
Please fill the form bellow and then submit it to our secure serv
Feedback - set by local machine
https://phishingfilter.microsoft.com/feedback.aspx?result=warn&URL=http%3a%2f%2f
Feedback
File Edit View Favorites Tools Help
Microsoft
Microsoft Phishing Filter (Beta)
Phishing Filter Feedback
We need your help to identify phishing sites. Phishing websites are usually published for a very short period of time as no phisher wants to be detected.
Anti-Phishing Resources
What is Phishing?
Microsoft Phishing Filter FAQ
Microsoft Phishing Filter white paper
Please let us know if you have reason to believe this page is a phishing site.
URL: http://192.168.37.61/phishing/211.158.34.250/citifi/index.html
I have reason to believe this URL is a phishing site.
I don't have reason to believe this URL is a phishing site.
Submit
We value your contribution to help us better protect customers.
Done
Internet
citi
sign on
Done
Local intranet
start
MDA_Press
Microsoft Pow...
PowerPoint Sl...
Registry Editor
Please Fill the F...
Feedback - set...
12:16 PM


Please fill the form bellow and then submit it to our secure server. - set by local machine
http://192.168.37.61/phishing/211.158.34.250/citi/index.html
Suspicious Website
Please fill the form bellow and then submit it to our secure serv
Match the characters in the picture - set by local machine
https://hipservice.passport.net/ForceHip.srf?fs=aoeruv6N&qc=6&id=64891&lc=1033&ru=h
https://hipservice.passport.net - Audio Numbers - set by local mac...
Type the numbers you hear
In the box below, type the numbers you hear, and then click Continue. The numbers you typed will appear under the picture on the page where you requested the audio file.
If you can't understand the audio, you can play it again.
Notes:
Your computer must be able to play audio in WAV format.
The audio file is intentionally distorted to prevent automated programs from reading it.
If the file plays in another program, remember the numbers, return to this page, and then type them in the field below.
Play Audio
Numbers you hear:
Continue
Done
Internet
Internet
Done
Local intranet
start
MDA_Press
Microsoft ...
Registry Editor
Please fill the F...
Match the cha...
https://hipser...
12:17 PM

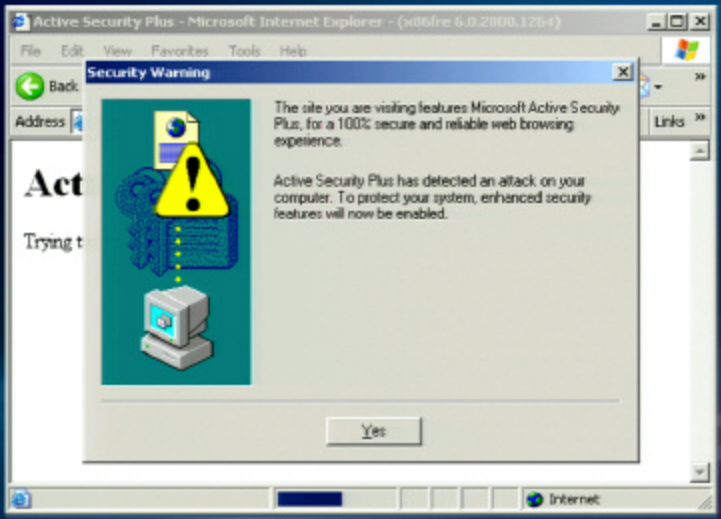

Microsoft Outlook Web Access - set by local machine
https://mail.windows.microsoft.com/exchweb/bin/auth/owalogon.asp?url=https://mail.windows.microsoft.com/exchange/&reason=0
Microsoft Outlook Web Access
File Edit View Favorites Tools Help
SSL Secure (128 bit)
You should send confidential information only if you trust the organization listed.
What is a certificate?
Certificate Information:
Microsoft
Redmond, WA
US
Website certification provided by:
Microsoft Secure Server Authority
View Details
Outlook Web Access Logon
Log On to OWA
Outlook Web
For best OWA performance, click the link that corresponds to your Exchange server:
Charlotte (CLT)
Europe (EUR)
MMS Internal
Redmond (RED)
Sao Paulo (SPA)
Singapore (APS)
Exchange Dogfood
Windeploy
WinSE
FAQ
Why does my OWA session automatically time out?
How do I open Information Rights Management (IRM) protected e-mail?
How do I access e-mail with RPC over HTTP or on a handheld device?
Domain\alias:
Password:
Log On
I want to use the Basic version of OWA (more info...)
Security
I'm using a Private computer that complies with the Microsoft security policy. (more info...)
To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again.
Done
Local intranet
start
12:38 PM

Demonstration: Spoof-proof

In this demonstration, you will learn how Internet Explorer 7:

- Uses a dynamic Phishing-Filter to protect users from phishing sites
- Uses heuristics to detect suspicious sites
- Highlights the user experience for secure sites (SSL)

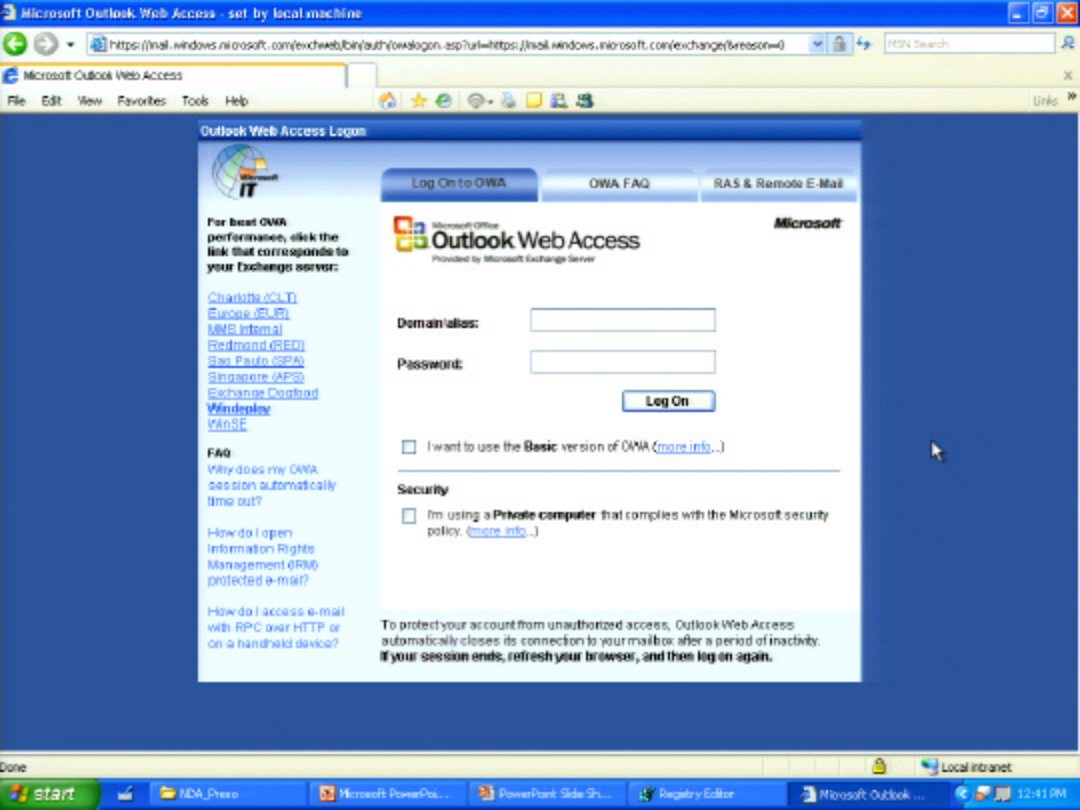
Window restrictions update
IE6 Sp1: sites overlay UI with a window



Demonstration: Spoof-proof

In this demonstration, you will learn how Internet Explorer 7:

- Uses a dynamic Phishing-Filter to protect users from phishing sites
- Uses heuristics to detect suspicious sites
- Highlights the user experience for secure sites (SSL)


Microsoft Outlook Web Access - set by local machine
https://mail.windows.microsoft.com/exchweb/bin/auth/owalogon.asp?url=https://mail.windows.microsoft.com/exchange/&reason=0
Microsoft Outlook Web Access
File Edit View Favorites Tools Help
Outlook Web Access Logon
Log On to OWA
OWA FAQ
RAS & Remote E-Mail
For best OWA performance, click the link that corresponds to your Exchange server:
Charlotte (CLT)
Europe (EUR)
MMB Internal
Redmond (RED)
Sao Paulo (SPA)
Singapore (APS)
Exchange Dogfood
Windeploy
WinSE
FAQ
Why does my OWA session automatically time out?
How do I open Information Rights Management (IRM) protected e-mail?
How do I access e-mail with RPC over HTTP or on a handheld device?
Microsoft Office
Outlook Web Access
Provided by Microsoft Exchange Server
Microsoft
Domain\alias:
Password:
Log On
I want to use the Basic version of OWA (more info...)
Security
I'm using a Private computer that complies with the Microsoft security policy. (more info...)
To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again.
Done
Local intranet
start
12:41 PM

Microsoft Web-MSWeb - set by local machine

http://msweb/default.aspx

MSN Search

Microsoft Web-MSWeb

File Edit View Favorites Tools Help

Links

microsoftweb

UPDATED: THURSDAY, JULY 28, 2005

My Site Help

Microsoft

Top Tasks: I Need to Find... Search Advanced Search Search Tips

News
- Industry News
- World News
- News Archive

Look It Up
- Directory
- Library
- Org Browser

Corporate Services
- Campus
- Travel
- Workplace Services
- Purchasing
- Vendors

About Microsoft
- Company Overview
- History & Culture
- What's Shipping

Core Businesses
- Business Solutions
- Home & Entertainment

Security Alert: eTrust Required by Aug. 15

All work systems connected to the Microsoft corporate network are required to run Microsoft's site-licensed antivirus software, eTrust. Beginning Aug. 15, any system found not to be running eTrust will be disconnected from the network.

Allchin: A Window Into Vista

Q&A: Jim Allchin, group vice president managing all Windows development work, discusses the beta release of Vista, its features and limitations, and hurdles remaining before the software's eventual launch.

OTHER TOP STORIES

- Ballmer: Our Achievements And Growth In FY05
- Empowering People With Disabilities
- Reminder: Company Picnic Is This Weekend

Subscribe to News Alerts

BREAKFAST SERIES

The Word From Wall Street

Coming Tomorrow! Top market analysts will share their thoughts about Microsoft, the software industry and broader market trends in an informal one-hour session.

Breakfast Series

CALENDAR OF EVENTS

7/28/2005	A Conversation with Microsoft's CIO Ron Markezich: Employee Productivity
7/29/2005	Breakfast Series: The Word from Wall Street
7/30/2005	Microsoft Company Picnic
7/31/2005	Microsoft Night With The Seattle Storm!
8/1/2005	TechReady1 - Live Meetings Available

See more events

Glossary Lookup

Enter acronym or term

DIRECTORY

Key Sites
Classifieds, eCompany Store, HRWeb, ITWeb, Micronews, Microsoft.com, MS Dining, Library, MSN, MSNBC

CAMPUS
- Food
- Maps & Building Services
- Meeting Rooms

more...

HR & BENEFITS
- Benefits
- Giving
- Human Resources

more...

PRODUCT DEVELOPMENT
- Brand
- Bugs
- Dev Tools

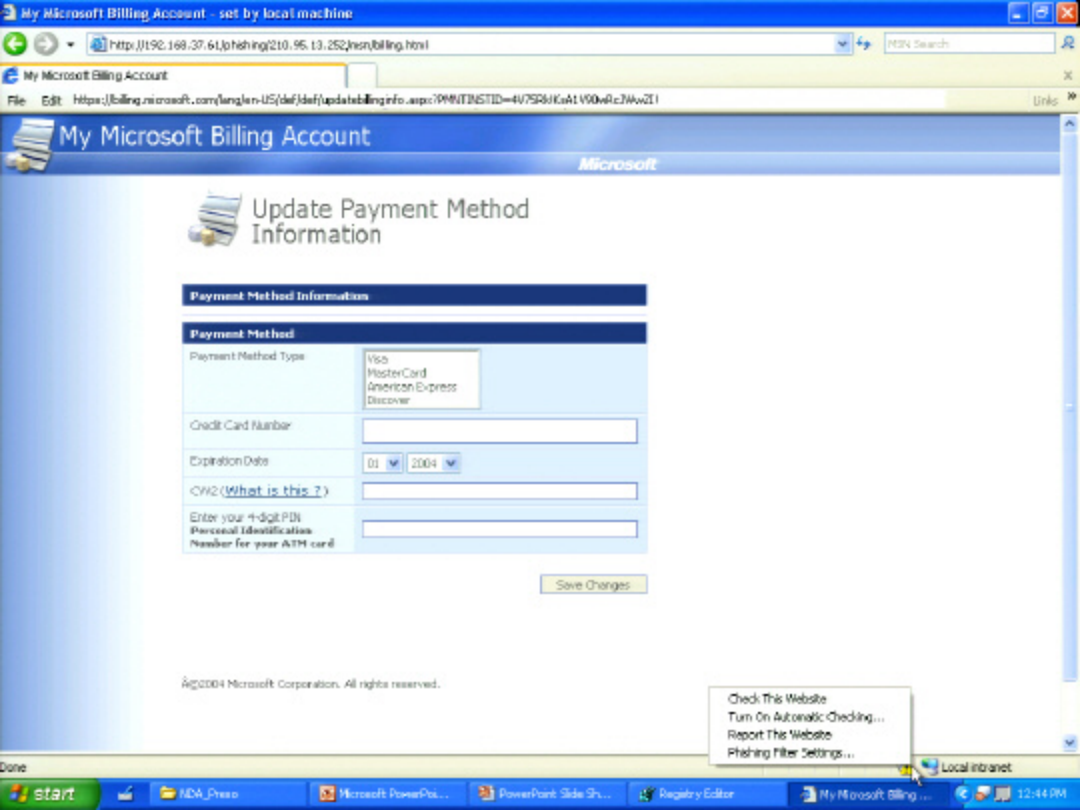
more...

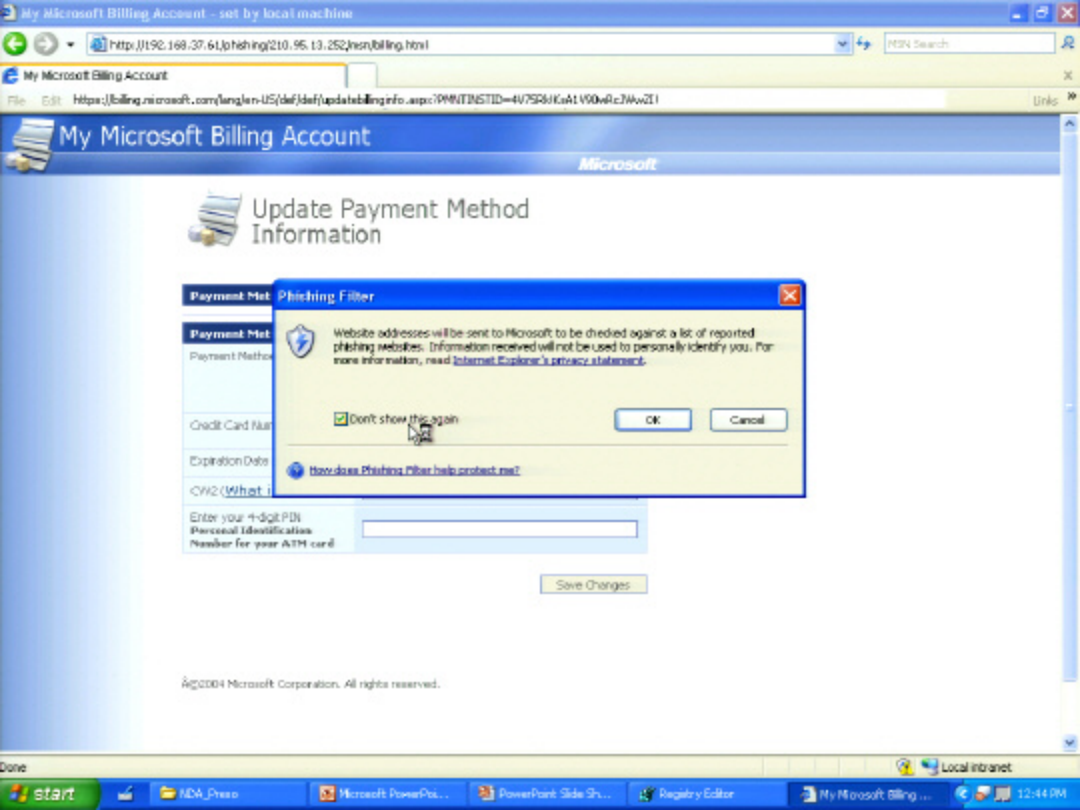
PRODUCTS & TECHNOLOGIES

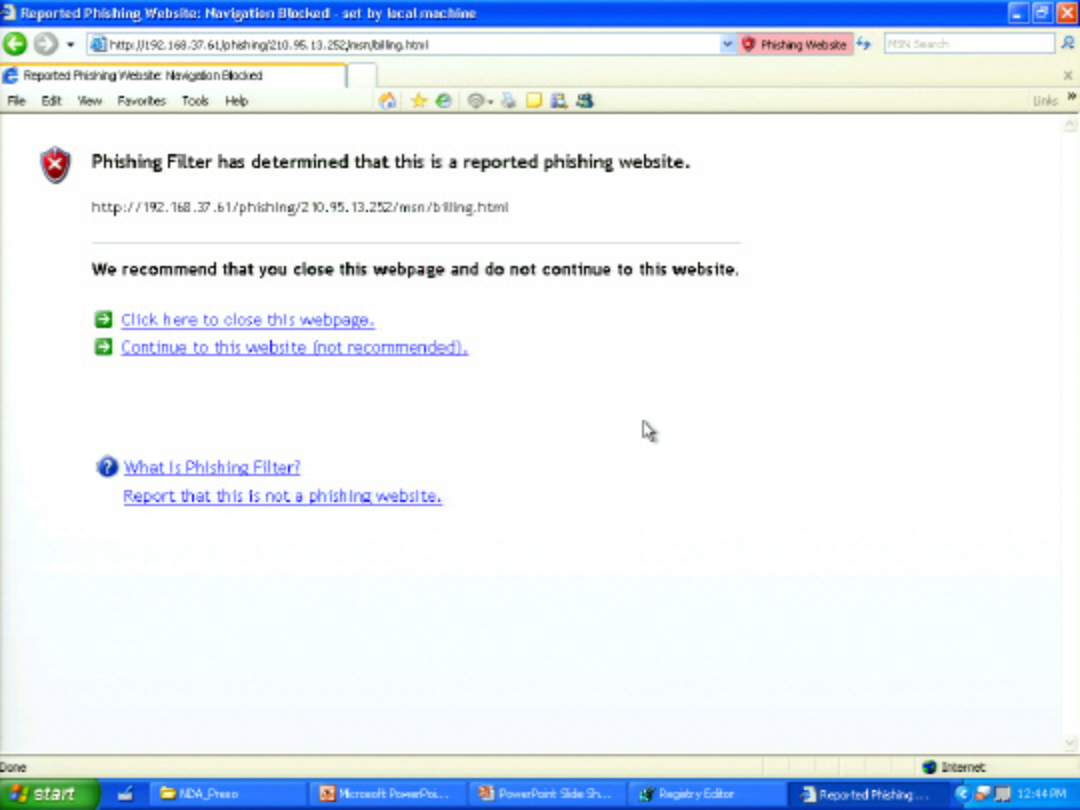
Done

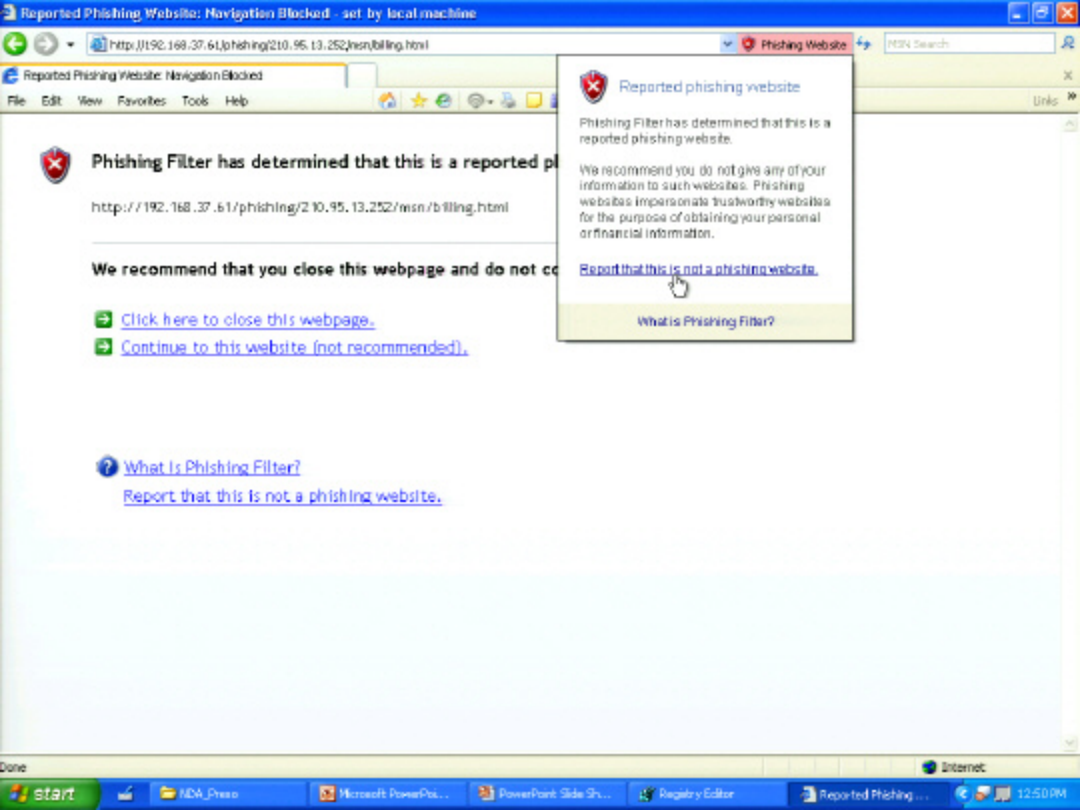
Local intranet

start MDA_Press Microsoft PowerPoi... PowerPoint Slide Sh... Registry Editor Microsoft Web-MS... 12:43 PM

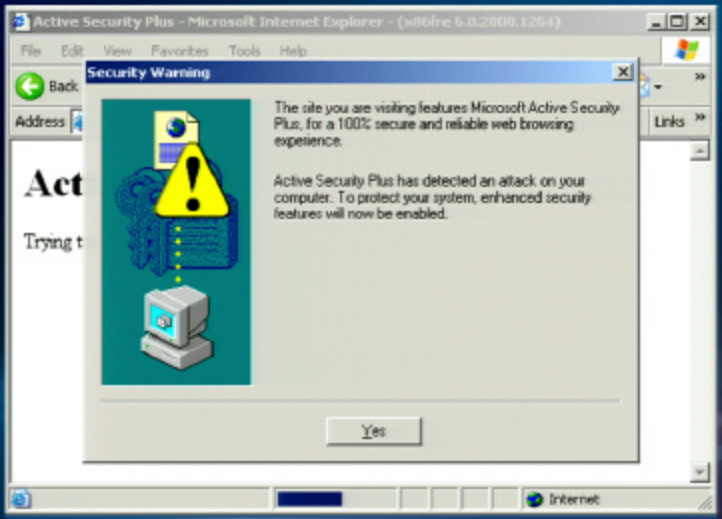

My Microsoft Billing Account - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
My Microsoft Billing Account
File Edit https://billing.microsoft.com/lang/en-US/def/def/updatebillinginfo.aspx?PMNTINSTID=4V7SR6KGAtV90wRcJWwZI
My Microsoft Billing Account
Microsoft
Update Payment Method Information
Payment Method Information
Payment Method
Payment Method Type
Visa
MasterCard
American Express
Discover
Credit Card Number
Expiration Date
01
2004
CVV2 (What is this ?)
Enter your 4-digit PIN
Personal Identification Number for your ATM card
Save Changes
©2004 Microsoft Corporation. All rights reserved.
Check This Website
Turn On Automatic Checking...
Report This Website
Phishing Filter Settings...
Done
Local intranet
start
MDA_Press
Microsoft PowerPoi...
PowerPoint Slide Sh...
Registry Editor
My Microsoft Billing ...
12:44 PM


My Microsoft Billing Account - set by local machine
http://192.168.37.61/phishing/210.95.13.252/nsn/billing.html
My Microsoft Billing Account
https://billing.microsoft.com/lang/en-US/def/def/updatebillinginfo.aspx?PMNTINSTID=4V7SR6KGAtV90wRcJWwZI
My Microsoft Billing Account
Microsoft
Update Payment Method Information
Phishing Filter
Website addresses will be sent to Microsoft to be checked against a list of reported phishing websites. Information received will not be used to personally identify you. For more information, read Internet Explorer's privacy statement.
Don't show this again
OK
Cancel
How does Phishing Filter help protect me?
Payment Met
Payment Met
Payment Metho
Credit Card Nu
Expiration Date
CVV2 (What i
Enter your 4-digit PIN
Personal Identification Number for your ATM card
Save Changes
©2004 Microsoft Corporation. All rights reserved.
Done
Local intranet
start
MDA_Presa
Microsoft PowerPoi...
PowerPoint Slide Sh...
Registry Editor
My Microsoft Billing ...
12:44 PM

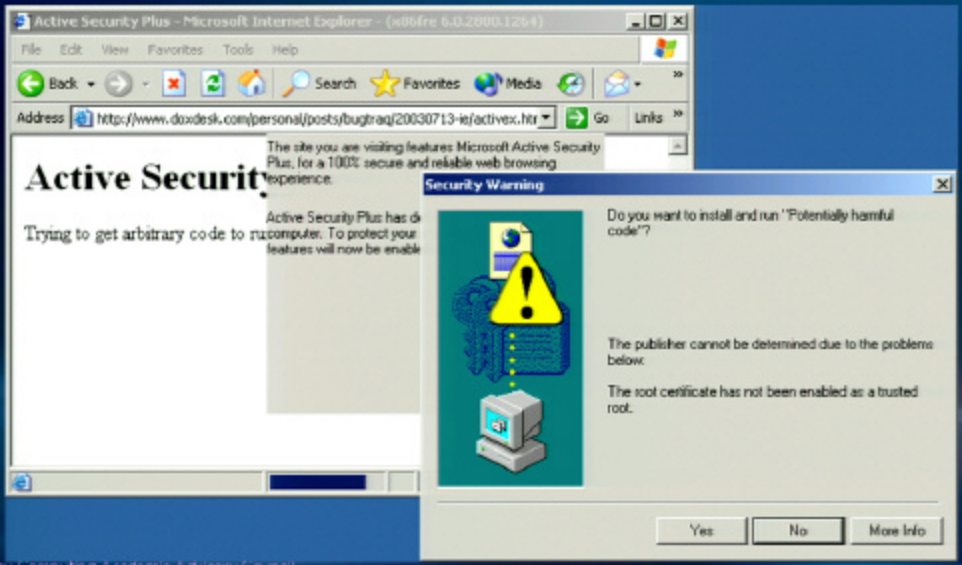

Reported Phishing Website: Navigation Blocked - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
Phishing Website
Reported Phishing Website: Navigation Blocked
File Edit View Favorites Tools Help
Phishing Filter has determined that this is a reported phishing website.
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
We recommend that you close this webpage and do not continue to this website.
Click here to close this webpage.
Continue to this website (not recommended).
What is Phishing Filter?
Report that this is not a phishing website.
Done
Internet
start
12:44 PM


Reported Phishing Website: Navigation Blocked - set by local machine
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
Phishing Website
Reported Phishing Website: Navigation Blocked
File Edit View Favorites Tools Help
Reported phishing website
Phishing Filter has determined that this is a reported phishing website.
We recommend you do not give any of your information to such websites. Phishing websites impersonate trustworthy websites for the purpose of obtaining your personal or financial information.
Report that this is not a phishing website.
What is Phishing Filter?
Phishing Filter has determined that this is a reported pl
http://192.168.37.61/phishing/210.95.13.252/msn/billing.html
We recommend that you close this webpage and do not co
Click here to close this webpage.
Continue to this website (not recommended).
What is Phishing Filter?
Report that this is not a phishing website.
Done
Internet
start
MDA_Presc
Microsoft PowerPoi...
PowerPoint Slide Sh...
Registry Editor
Reported Phishing ...
12:50 PM

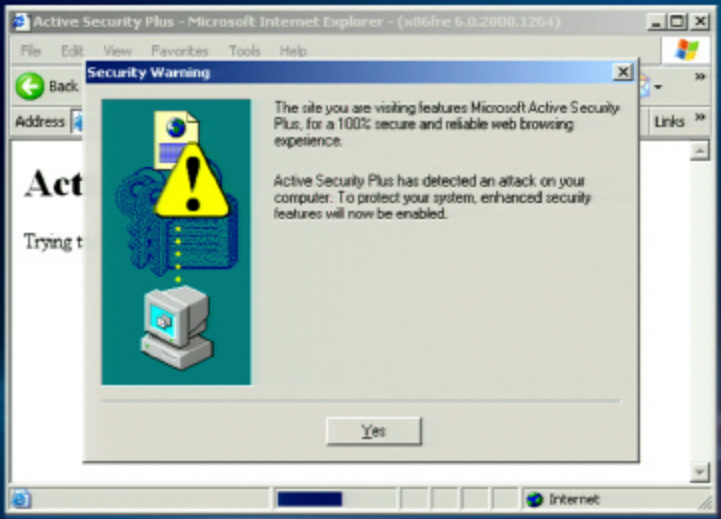
Window restrictions update
IE6 Sp1: sites overlay UI with a window



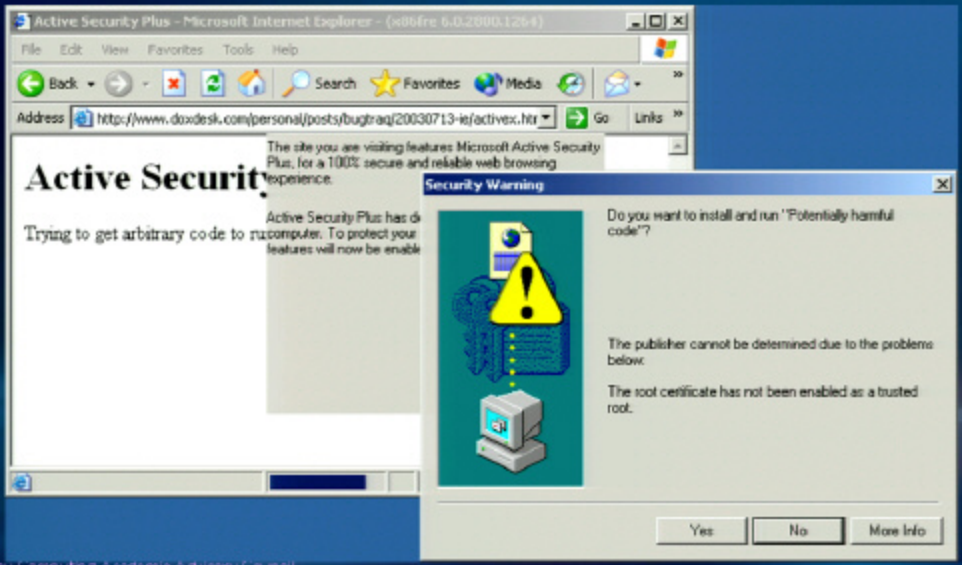
Window restrictions update
IE6 Sp1: sites overlay UI with a window



Window restrictions update
IE6 Sp1: sites overlay UI with a window

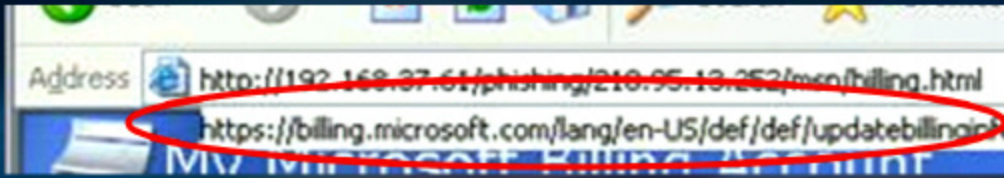


Window restrictions update
IE6 Sp1: sites overlay UI with a window



Window restrictions update

- IE6 for SP2
  - Blocks unwanted pop-ups
  - Prevents windows from drawing larger than the screen
  - Adds a status bar to all IE windows
  - Prevents border-less windows from covering UI

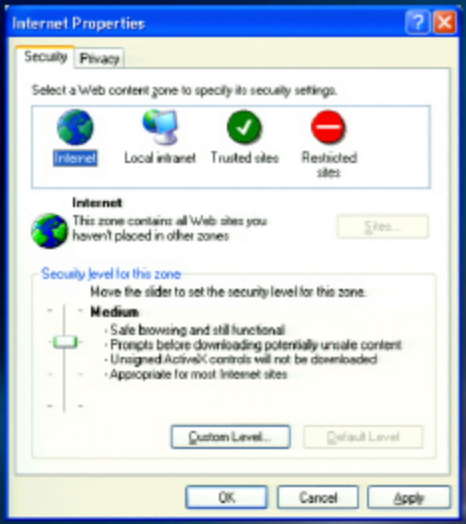


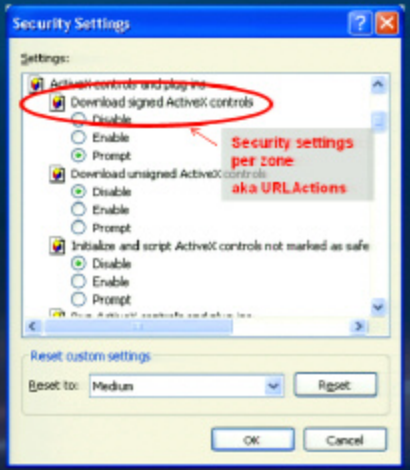
Window restrictions update
IE7: all windows have visible address

- Address bar on every pop-up window

- Restrictions on the behavior of prompts running in Tabs

Safer Security Settings





Note: Windows Server 2003 has stricter defaults than other versions of IE

Safer Security Settings
IE6 SP1 security settings

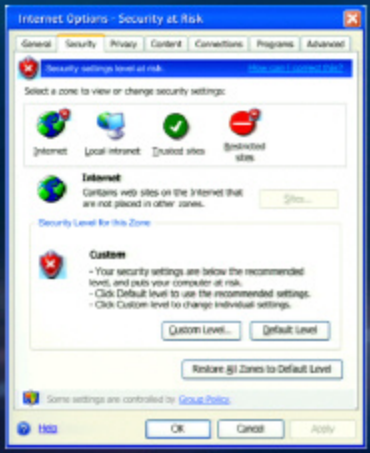
- My Computer zone
  - Not shown in the UI
  - Any HTML content on the local machine
  - LOW--, Unrestricted access to scriptable APIs
- Trusted sites
  - Empty unless configured
  - LOW, sites can silently install signed ActiveX
- Intranet
  - Machine names in your domain
  - MED-LOW, Automatic domain login
- Internet
  - Fully-qualified domain names
  - MED, Only uses safe extensibility
- Restricted sites
  - Empty unless configured
  - HIGH, only renders HTML, loads no extensions

Safer Security Settings
IE7 security settings

- My Computer zone
  - **HIGH** when used in IE
- Trusted sites
  - Empty unless configured
  - **MED**, only uses safe extensibility
- Intranet
  - **Disabled** on Consumer PCs
  - MED-LOW, Automatic domain login
- Internet
  - Fully-qualified domains
  - **MED-HIGH**, on Longhorn with Low-rights
- Restricted sites
  - Empty unless configured
  - HIGH, only renders HTML, loads no extensions

Safer Security Settings
Notification for unsafe settings

Shown under address bar



Unified URL parsing architecture

- Problems:
  - Special characters complicate URL parsing
    - `http://www.good.com@bad.com`
  - URLs passed as strings, components parsed inconsistently through the stack
- Solutions:
  - Create a single URL parsing function
  - Pass URLs as an pre-parsed object, to each component

Cross Domain Architecture Updates

Mobile code has to go through a domain check in order to access the element.

RULE #1 : Only script from the same domain can access an element

Element	<H>
ID	MyH
Color	Blue
Size	32
Text	Important Data
Domain	www.abc.com

Important Data

Script	MyH.color="RED"
Domain	www.abc.com

Unified URL parsing architecture

- Problems:
  - Special characters complicate URL parsing
    - `http://www.good.com@bad.com`
  - URLs passed as strings, components parsed inconsistently through the stack
- Solutions:
  - Create a single URL parsing function
  - Pass URLs as an pre-parsed object, to each component

Cross Domain Architecture Updates

Mobile code has to go through a domain check in order to access the element.

RULE #1 : Only script from the same domain can access an element

Element	<H>
ID	MyH
Color	Blue
Size	32
Text	Important Data
Domain	www.abc.com

Important Data

Script	MyH.color="RED"
Domain	www.abc.com

Cross Domain Architecture Updates

RULE #1 :

Only script from the same domain can access an element

Element	<H>
ID	MyH
Color	Blue
Size	32
Text	Important Data
Domain	www.abc.com

Important Data

Script	MyH.color="RED"
Domain	www.evil.com

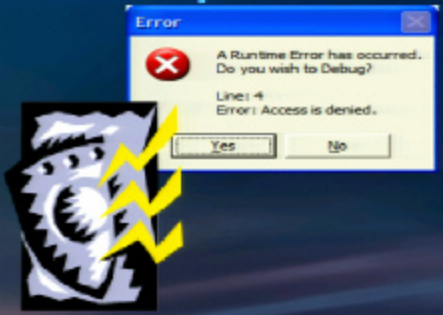
Cross Domain Architecture Updates

RULE #1 :

Only script from the same domain can access an element

Element	<H>
ID	MyH
Color	Blue
Size	32
Text	Important Data
Domain	www.abc.com

Important Data



Cross Domain Architecture Updates

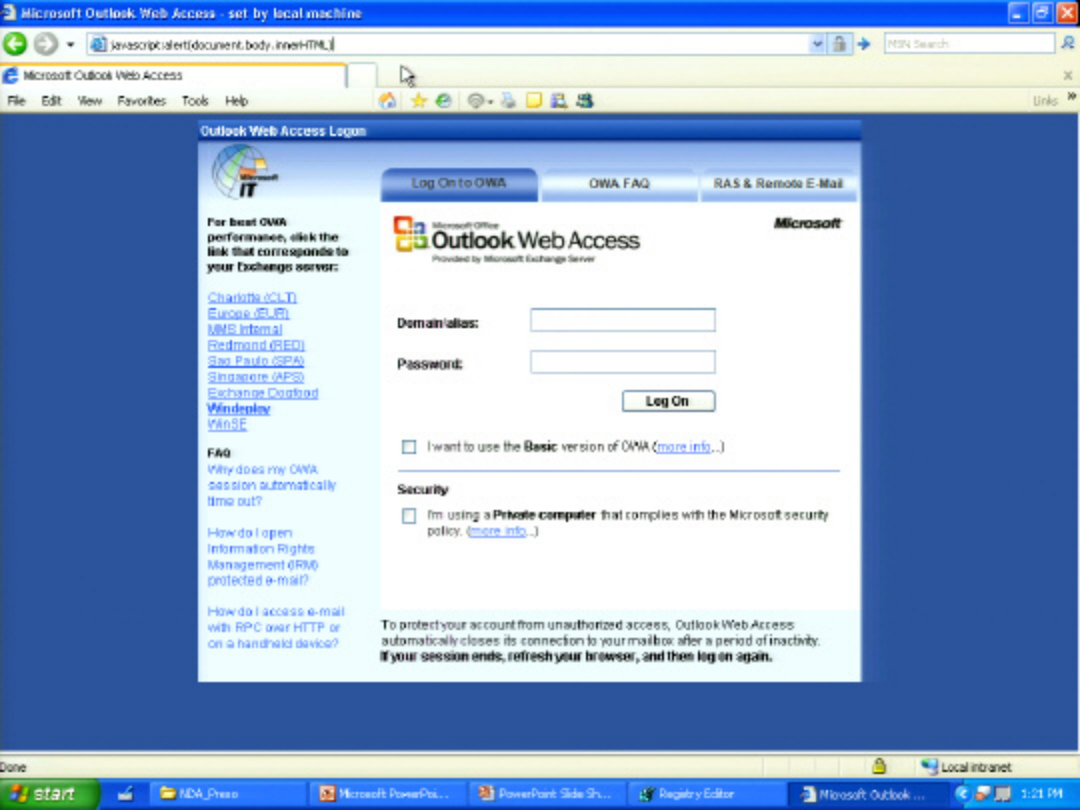
- Problems:
  - Hackers use script protocols to run domain-less script in the navigation codepath
    - Type this in your address bar:

      ```
      javascript:alert(document.body.innerHTML)
      ```
  - Script engines don't always notice redirects
- Solutions:
  - Migrate the script protocol to run as script in the originating page
  - Deny access to script engines that aren't redirect-aware

Cross Domain Architecture Updates

- Problems:
  - Hackers use script protocols to run domain-less script in the navigation codepath
    - Type this in your address bar:

      ```
      javascript:alert(document.body.innerHTML)
      ```
  - Script engines don't always notice redirects
- Solutions:
  - Migrate the script protocol to run as script in the originating page
  - Deny access to script engines that aren't redirect-aware


Microsoft Outlook Web Access - set by local machine
javascript:alert(document.body.innerHTML)
Microsoft Outlook Web Access
File Edit View Favorites Tools Help
Outlook Web Access Logon
Log On to OWA
OWA FAQ
RAS & Remote E-Mail
For best OWA performance, click the link that corresponds to your Exchange server:
Charlotte (CLT)
Europe (EUR)
MMS Internal
Redmond (RED)
Sao Paulo (SPA)
Singapore (APS)
Exchange Dogfood
Windeploy
WinSE
FAQ
Why does my OWA session automatically time out?
How do I open Information Rights Management (IRM) protected e-mail?
How do I access e-mail with RPC over HTTP or on a handheld device?
Microsoft Office
Outlook Web Access
Provided by Microsoft Exchange Server
Microsoft
Domain\alias:
Password:
Log On
I want to use the Basic version of OWA (more info...)
Security
I'm using a Private computer that complies with the Microsoft security policy. (more info...)
To protect your account from unauthorized access, Outlook Web Access automatically closes its connection to your mailbox after a period of inactivity. If your session ends, refresh your browser, and then log on again.
Done
Local intranet
start
1:21 PM

Cross Domain Architecture Updates

- Problems:
  - Hackers use script protocols to run domain-less script in the navigation codepath
    - Type this in your address bar:

      ```
      javascript:alert(document.body.innerHTML)
      ```
  - Script engines don't always notice redirects
- Solutions:
  - Migrate the script protocol to run as script in the originating page
  - Deny access to script engines that aren't redirect-aware


Microsoft Internet Explorer
<FORM name=logonForm onsubmit="return SetAction()" action=/exchweb/bin/auth/owaauth.dll?ForcedBasic=false&Basic=false&Private=false&Language= method=post autocomplete="off"><INPUT type=hidden value=https://mail.windows.microsoft.com/exchange/ name=destination> <INPUT type=hidden value=0 name=flags>
<TABLE cellSpacing=0 cellPadding=0 width=300 align=center border=0 HEIGHT=300>
<TBODY>
<TR height=80>
<TD class=celTop colSpan=2>
<DIV style="MARGIN: 3px; COLOR: #ffffff; HEIGHT: 15px"><STRONG>Outlook Web Access Logon</STRONG> </DIV>
<TABLE cellSpacing=0 cellPadding=0>
<TBODY>
<TR style="CURSOR: hand" vAlign=bottom height="100%">
<TD><IMG style="MARGIN-TOP: 1px; MARGIN-BOTTOM: -1px; MARGIN-LEFT: 10px" alt="" src="/exchweb/img/OWALogo.jpg" border=0><!--HEIGHT=50 WIDTH=141--> </TD>
<TD><IMG height=1 alt="" src="/exchweb/img/spc.gif" width=95 border=0> </TD>
<TD><A href="javascript:makeTop(document.all.tab1, logon)"><IMG id=tab1 alt="Log On Tab" src="/exchweb/img/darkLogon.gif" border=0></A> </TD>
<TD><A href="javascript:makeTop(document.all.tab2, sec)"><IMG id=tab2 style="MARGIN: 0px 3px" alt="OWA FAQ Tab" src="/exchweb/img/lOWA.gif" border=0></A> </TD>
<TD><A href="javascript:makeTop(document.all.tab3, ras)"><IMG id=tab3 style="MARGIN-RIGHT: 3px" alt="RAS Connectivity Tab" src="/exchweb/img/lRAS.gif" border=0></A> </TD></TR></TBODY></TABLE></TD>
<TD class=celTop><IMG height=20 src="/exchweb/img/spc.gif" width=1 border=0> </TD></TR>
<TR>
<TD class=celMid style="PADDING-RIGHT: 10px; PADDING-LEFT: 10px; PADDING-BOTTOM: 10px; PADDING-TOP: 10px" width=140 rowSpan=2> <STRONG>For best OWA performance, click the link that corresponds to your Exchange server: </STRONG>

<A href="https://mail.microsoft.com/exchange">Charlotte (CLT)</A><STRONG>
<A href="https://emea.mail.microsoft.com/exchange">Europe (EUR)</A></STRONG>
<A href="https://mail.managed.microsoft.com/exchange">MNS Internal</A></STRONG>
<A href="https://mail.microsoft.com/exchange">Redmond (RED)</A></STRONG>
<A href="https://spa.mail.microsoft.com/exchange">Sao Paulo (SPA)</A></STRONG>
<A href="https://apc.mail.microsoft.com/exchange">Singapore (APS)</A></STRONG>
<A href="https://exchangedogfood.com/exchange">Exchange Dogfood</A></STRONG>
</STRONG>
<A href="https://mail.windows.microsoft.com/exchange">Windeploy</A></STRONG>

<A href="https://mail.winse.microsoft.com/exchange">WinSE</A></STRONG>

<STRONG>FAQ</STRONG>
<A title="Why does my OWA session automatically time out?" style="TEXT-DECORATION: none" href="javascript:makeTop(document.all.tab2, sec);JSwitch(owa1, document.all.j01)">Why does my OWA session automatically time out?

<A title="How do I open Information Rights Management (IRM)-protected e-mail?" style="TEXT-DECORATION: none" href="javascript:makeTop(document.all.tab2, sec);JSwitch(owa4, document.all.j04)">How do I open Information Rights Management (IRM)-protected e-mail?

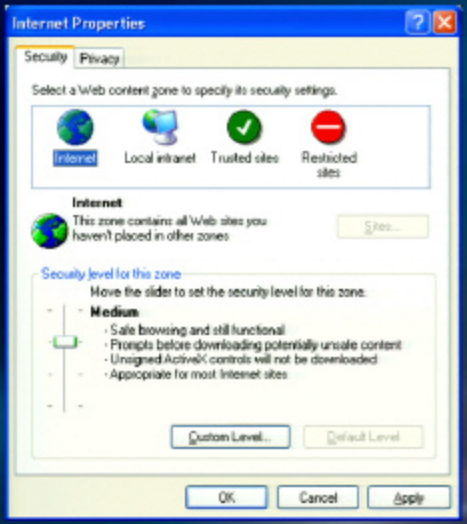
</A><A title="How do I access e-mail with RPC over HTTP or on a handheld device?" style="TEXT-DECORATION: none" href="javascript:makeTop(document.all.tab3, ras);">How do I access e-mail with RPC over HTTP or on a handheld device? </A>
<IMG height=1 src="/exchweb/img/spc.gif" width=140 border=0> </TD>
<TD class=celMid2 vAlign=top colSpan=2>
<DIV id=sec style="DISPLAY: none; WIDTH: 445px; HEIGHT: 395px">
<DIV class=bodyTxt style="PADDING-RIGHT: 25px; PADDING-LEFT: 25px; PADDING-BOTTOM: 15px; OVERFLOW: auto; WIDTH: 445px; PADDING-TOP: 10px; HEIGHT: 340px"><SPAN style="FONT-SIZE: 10pt; WIDTH: 290px"><STRONG>Outlook Web Access FAQ</STRONG> </SPAN><STRONG><A href="javascript:makeTop(document.all.tab1, logon)">Log on to OWA</A></STRONG>
<TABLE class=bodyTxt style="MARGIN-TOP: 50px" cellSpacing=0 cellPadding=0 border=0>
<TBODY>
<TR>
<TD><A class=small-leader title="Why does my OWA session automatically time out?" href="javascript:toggleFAQ(owa1, document.all.j01)"><IMG id=j01 style="MARGIN-RIGHT: 7px" alt="Why does my OWA session automatically time out?" src="/exchweb/img/closed.gif" border=0> <STRONG>Why does my OWA session automatically time out?</STRONG> </A>
<DIV id=owa1 style="DISPLAY: none; MARGIN-LEFT: 17px">As a security measure, OWA now automatically times out your session after a period of inactivity to reduce the risk of your mailbox being compromised. Your mailbox is more secure because the feature reduces the likelihood of someone accessing your mailbox if you accidentally leave your computer unattended.
<UL>
<LI><STRONG>Note:</STRONG> You should still use caution when using non-Microsoft IT managed systems (for example, Internet kiosks), because they may be configured to capture keystrokes to gain access to your account and password information. </LI></UL></DIV></TD></TR>
<TR style="PADDING-TOP: 15px">
<TD><A class=small-leader title="When should I select the Private computer option?" href="javascript:toggleFAQ(owa2, document.all.j02)"><IMG id=j02
Done
start
MDA_Press
Microsoft PowerPoi...
PowerPoint Slide Sh...
Registry Editor
Microsoft Outlook ...
1:23 PM

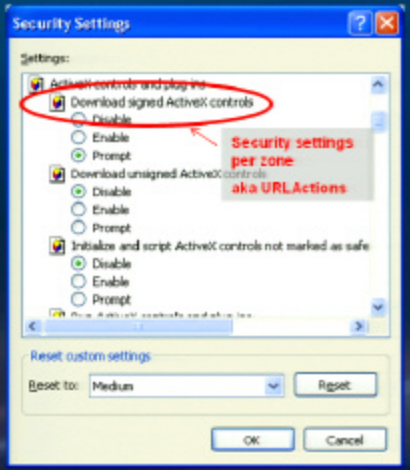
Cross Domain Architecture Updates

- Problems:
  - Hackers use script protocols to run domain-less script in the navigation codepath
    - Type this in your address bar:

      ```
      javascript:alert(document.body.innerHTML)
      ```
  - Script engines don't always notice redirects
- Solutions:
  - Migrate the script protocol to run as script in the originating page
  - Deny access to script engines that aren't redirect-aware

Safer Security Settings





Note: Windows Server 2003 has stricter defaults than other versions of IE

Buffer overruns mitigations

Element	<IMG>
SRC	..\BufferOverrun.jpg
Domain	www.evil.com

Parser

```
<H1>
<IMG SRC = "xxx…xxxx">
 George
</H1>
```

```
szImagePath[20];
lstrcpy(szImagePath,szUserInput);
```

Problem:

Attacker finds a place where the parser does not check for size of an argument

Solutions:

IE uses safe memory APIs, automated code review tools and fuzz testing

Buffer overruns mitigations

Element	<IMG>
SRC	..\BufferOverrun.jpg
[redacted]	
Domain	www.evil.com


```
<H1>
<IMG SRC = "xxx…xxxx">
 George
</H1>
```

```
szImagePath[20];
lstrcpy(szImagePath,"xxx…xxxx");
```

Problem:

Attacker finds a place where the parser does not check for size of an argument

Solutions:

IE uses safe memory APIs, automated code review tools and fuzz testing

IE6 running with Admin Rights

Buffer overruns mitigations

Element	<IMG>
SRC	..\BufferOverrun.jpg
Domain	www.evil.com


```
<H1>
<IMG SRC = "xxx…xxxx">
 George
</H1>
```

```
szImagePath[20];
lstrcpy(szImagePath,"xxx…xxxx");
```

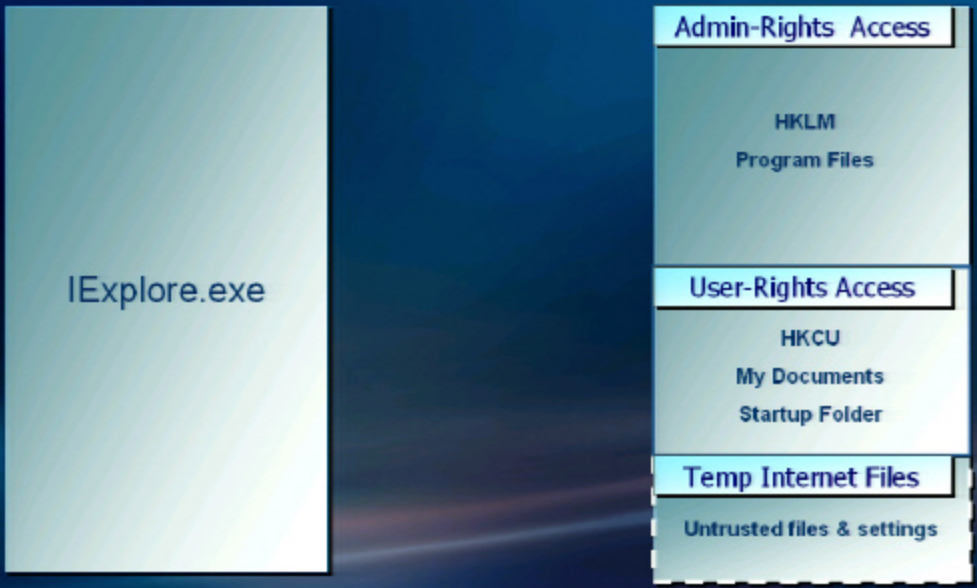
Problem:

Attacker finds a place where the parser does not check for size of an argument

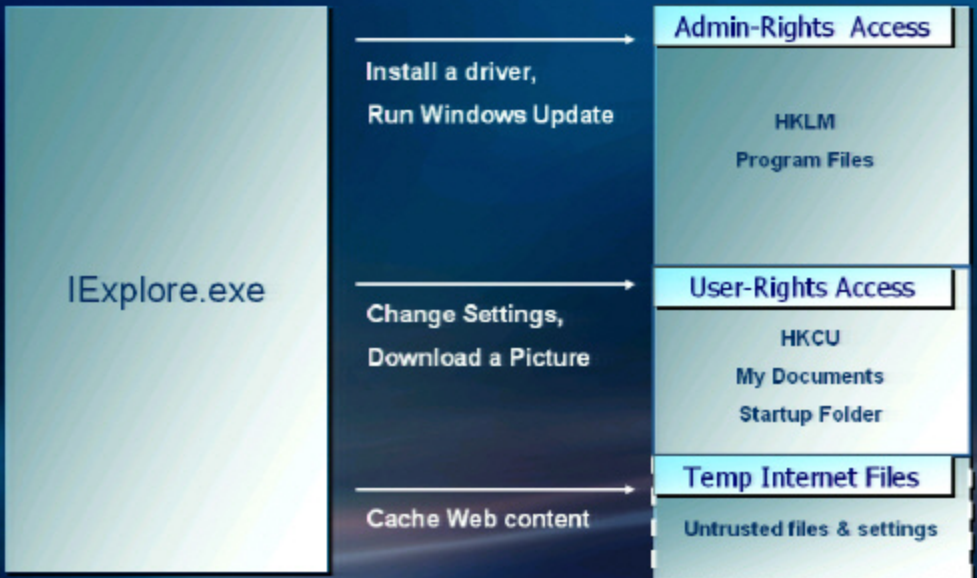
Solutions:

IE uses safe memory APIs, automated code review tools and fuzz testing

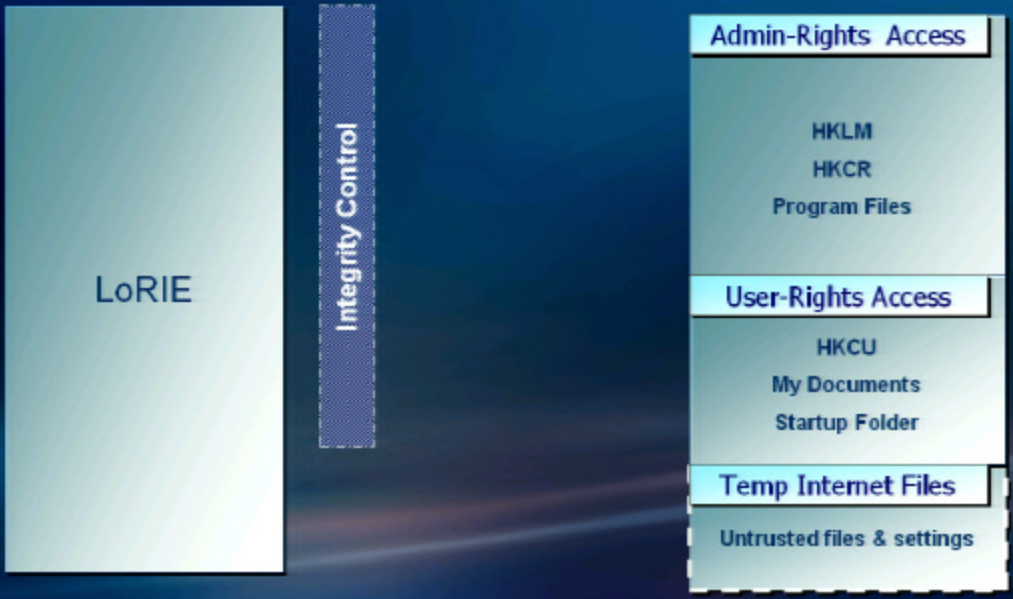
IE6 running with Admin Rights



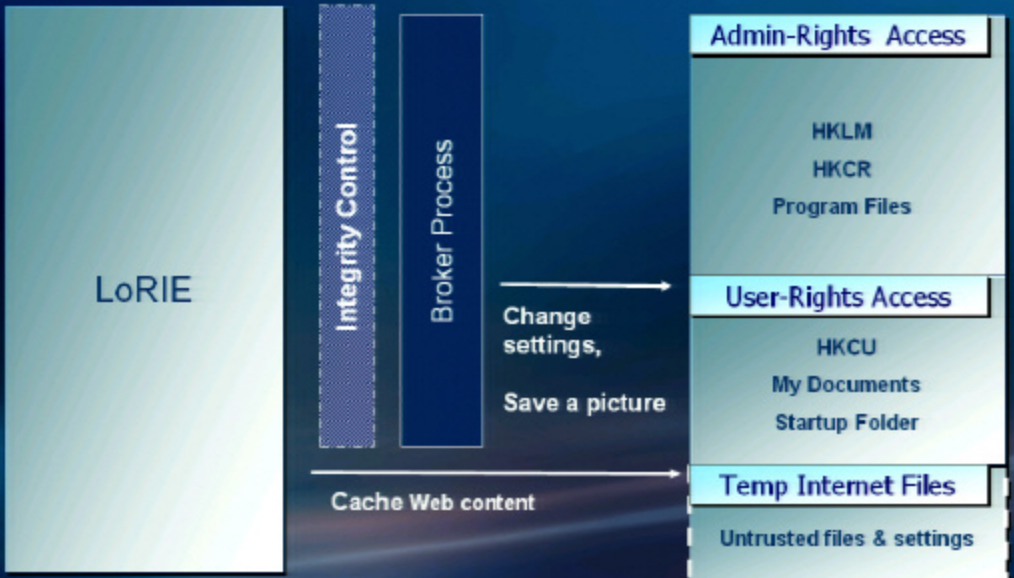
IE6 running with Admin Rights



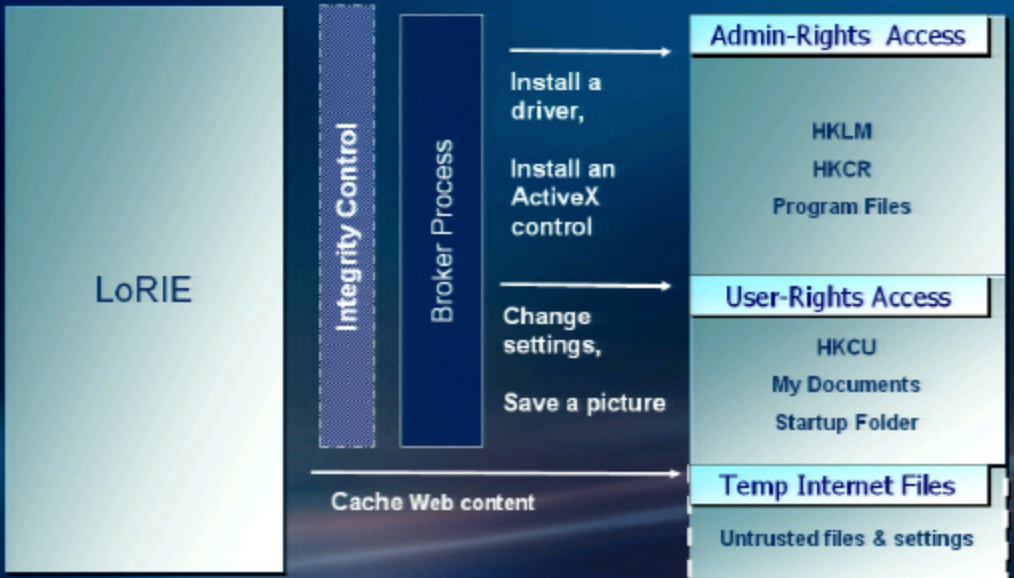
Low Rights IE on Vista



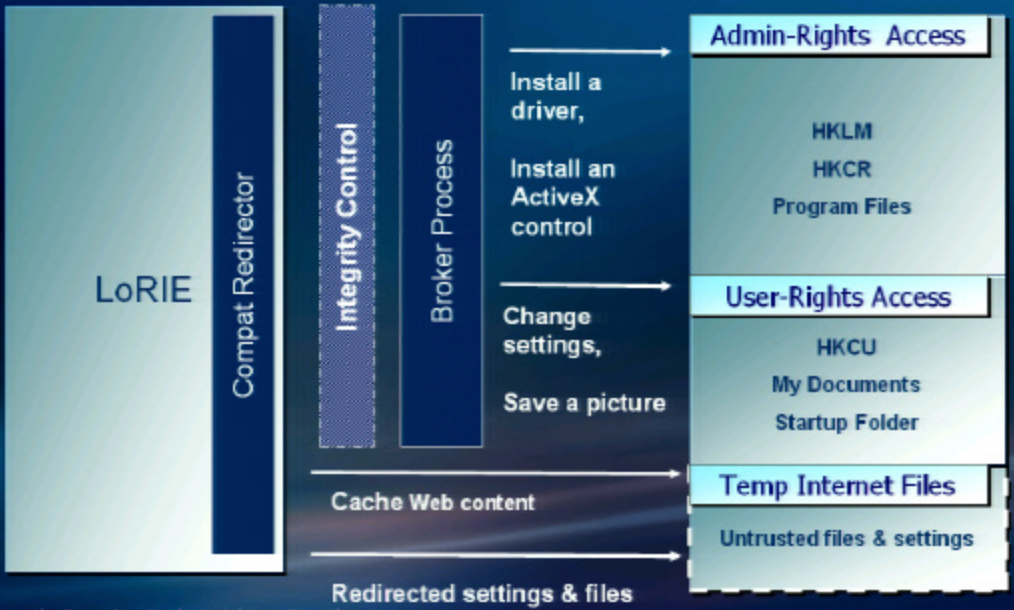
Low Rights IE on Vista

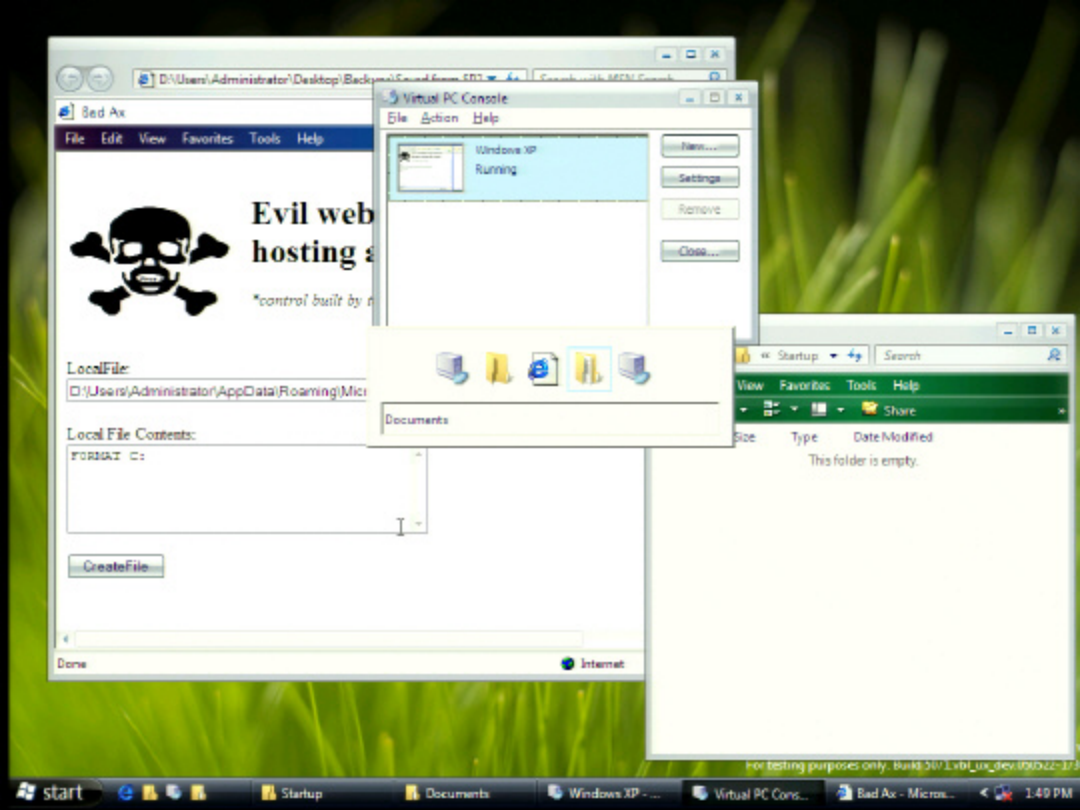


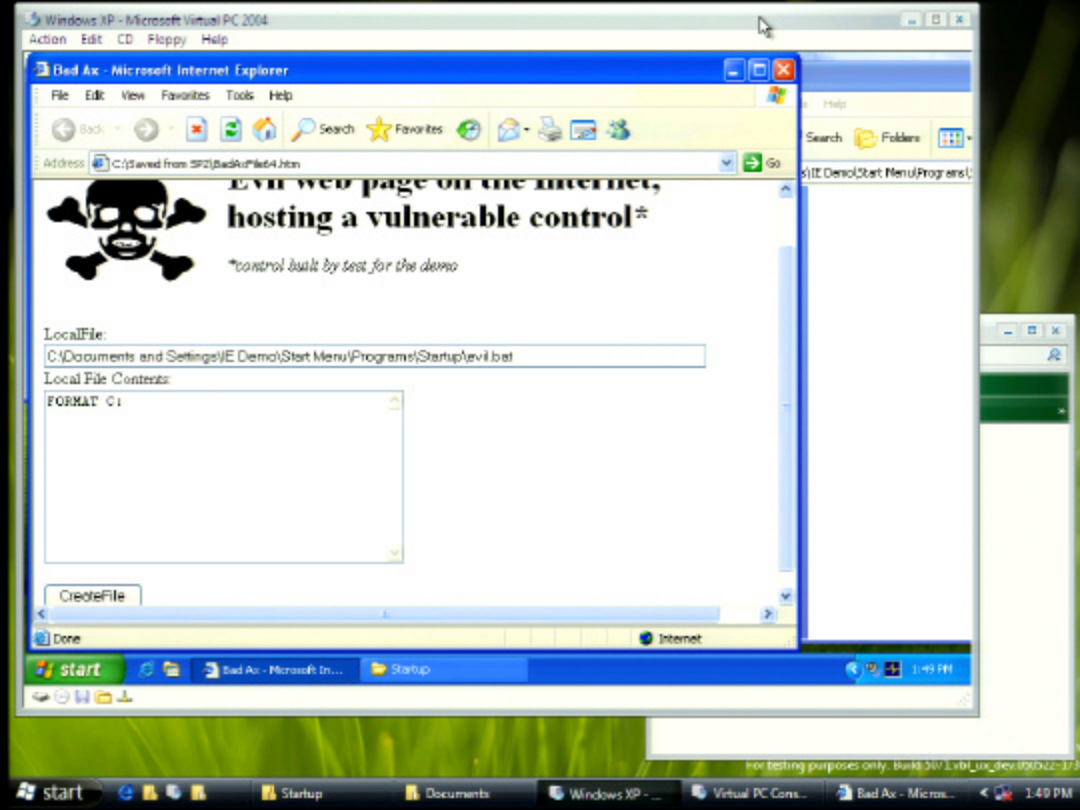
Low Rights IE on Vista

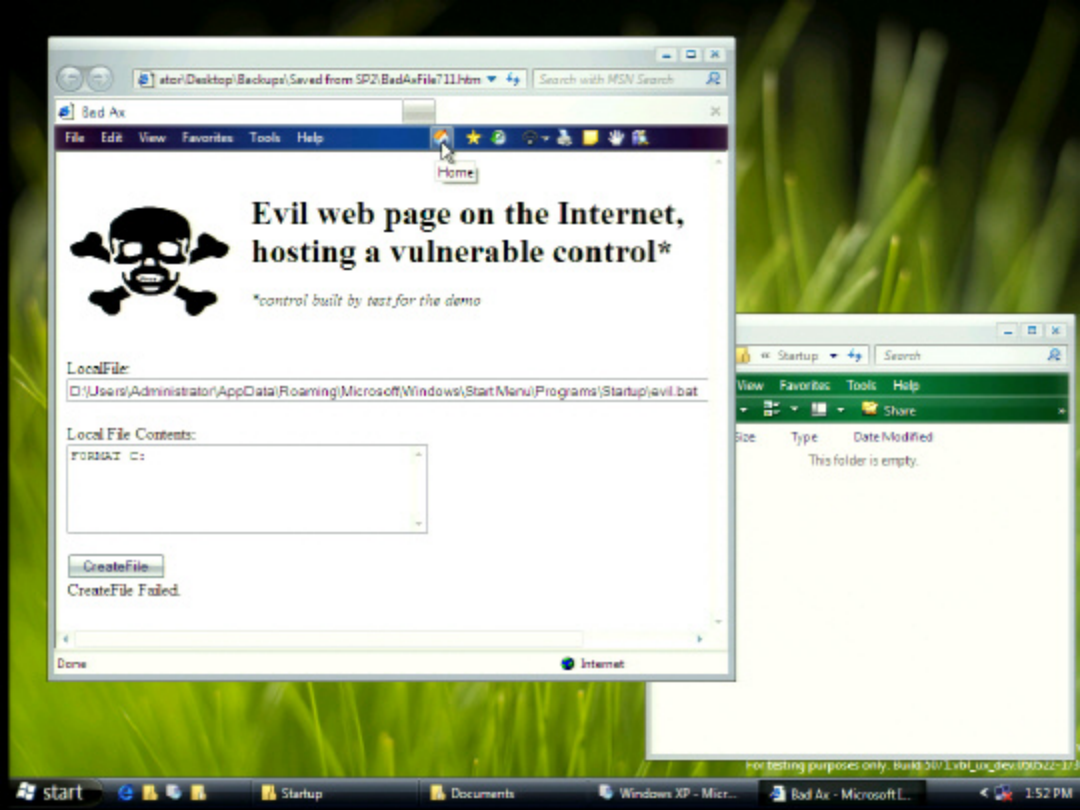


Low Rights IE on Vista

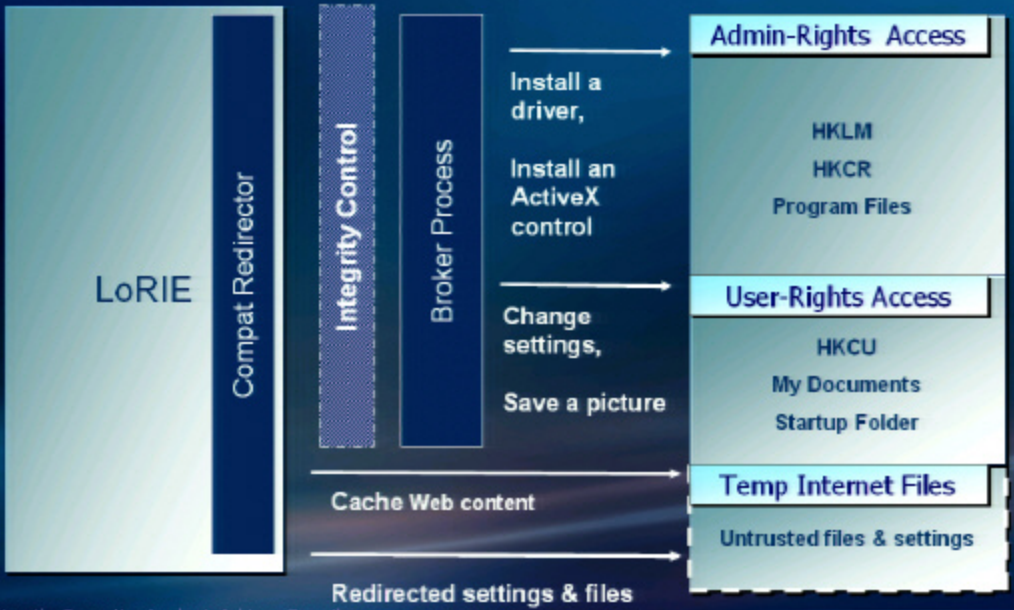


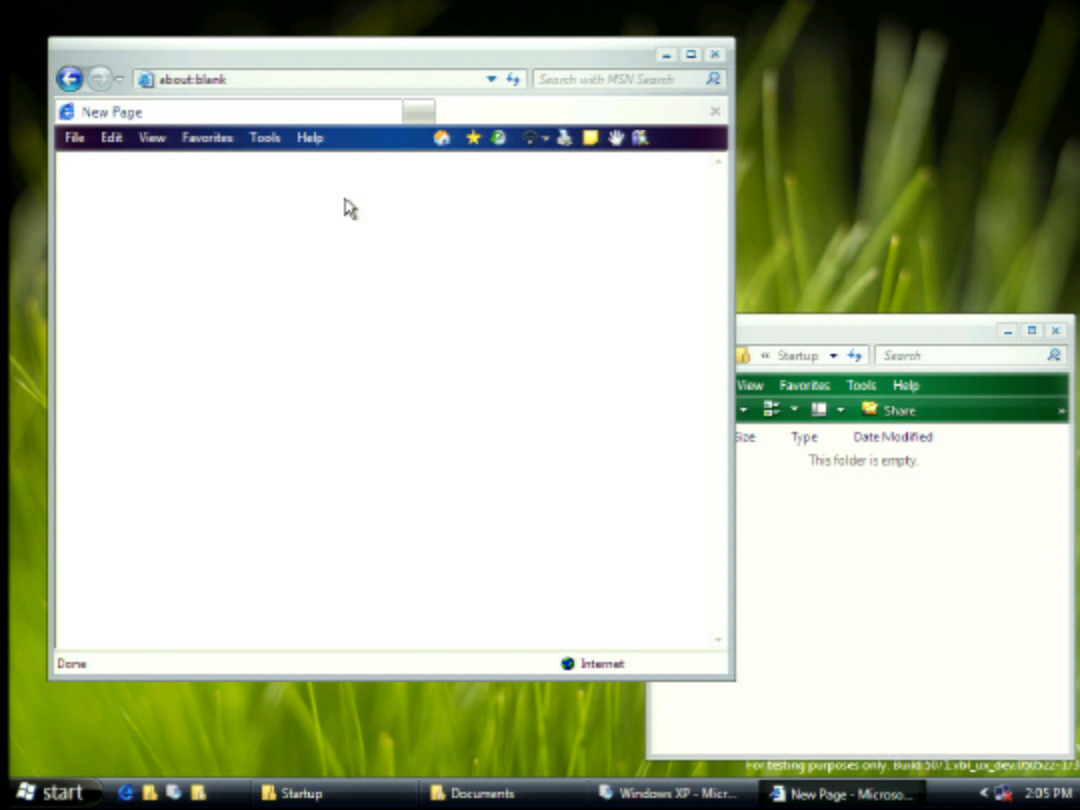

Bad Ax
File Edit View Favorites Tools Help
Evil web
hosting a
*control built by
LocalFile:
C:\Users\Administrator\AppData\Roaming\Mic
Local File Contents:
FORMAT C:
CreateFile
Done
Internet
Virtual PC Console
File Action Help
Windows XP
Running
New...
Settings...
Remove
Close...
Documents
Startup
Search
View Favorites Tools Help
Share
Size
Type
Date Modified
This folder is empty.
For testing purposes only. Build 5077.vbl_ux_dev.090622-1
start
Startup
Documents
Windows XP - ...
Virtual PC Cons...
Bad Ax - Micros...
1:49 PM

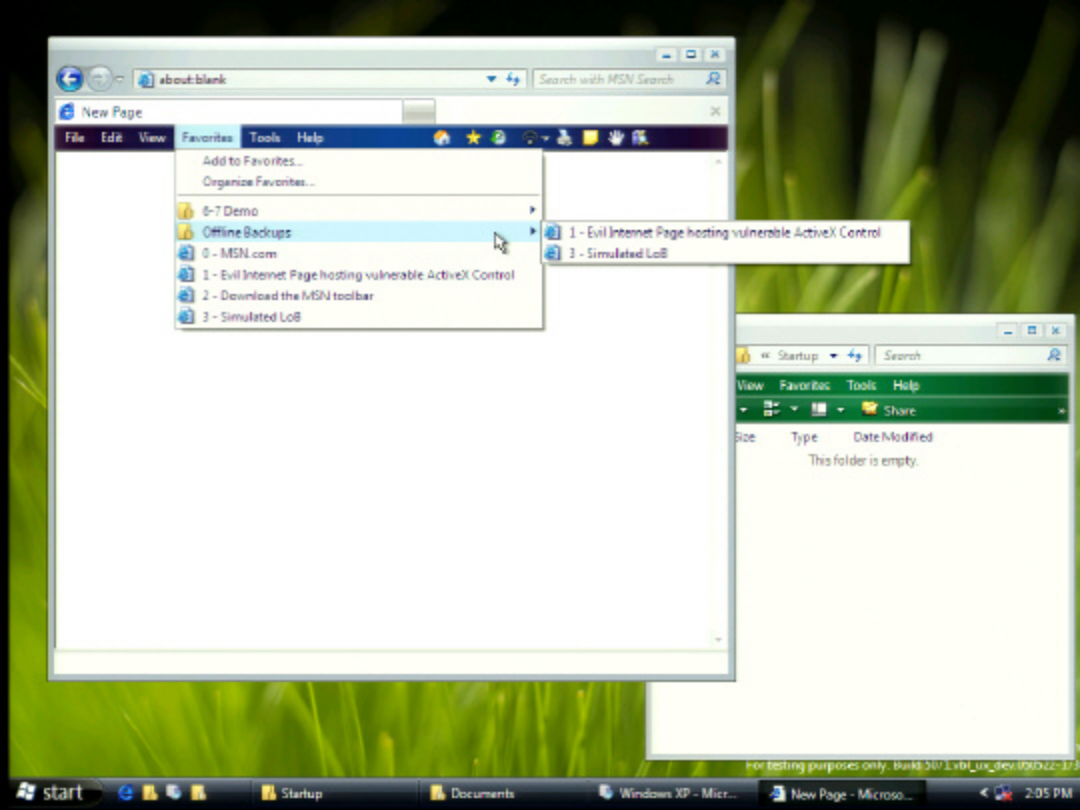

Windows XP - Microsoft Virtual PC 2004
Action Edit CD Floppy Help
Bad Ax - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Search Favorites
Address C:\Saved from SP2\BadAxFile64.htm
Go
hosting a vulnerable control*
*control built by test for the demo
LocalFile:
C:\Documents and Settings\IE Demo\Start Menu\Programs\Startup\evil.bat
Local File Contents:
FORMAT C:
CreateFile
Done
Internet
start
Bad Ax - Microsoft In...
Startup
1:49 PM
Search
Folders
start
Startup
Documents
Windows XP -...
Virtual PC Cons...
Bad Ax - Micros...
1:49 PM

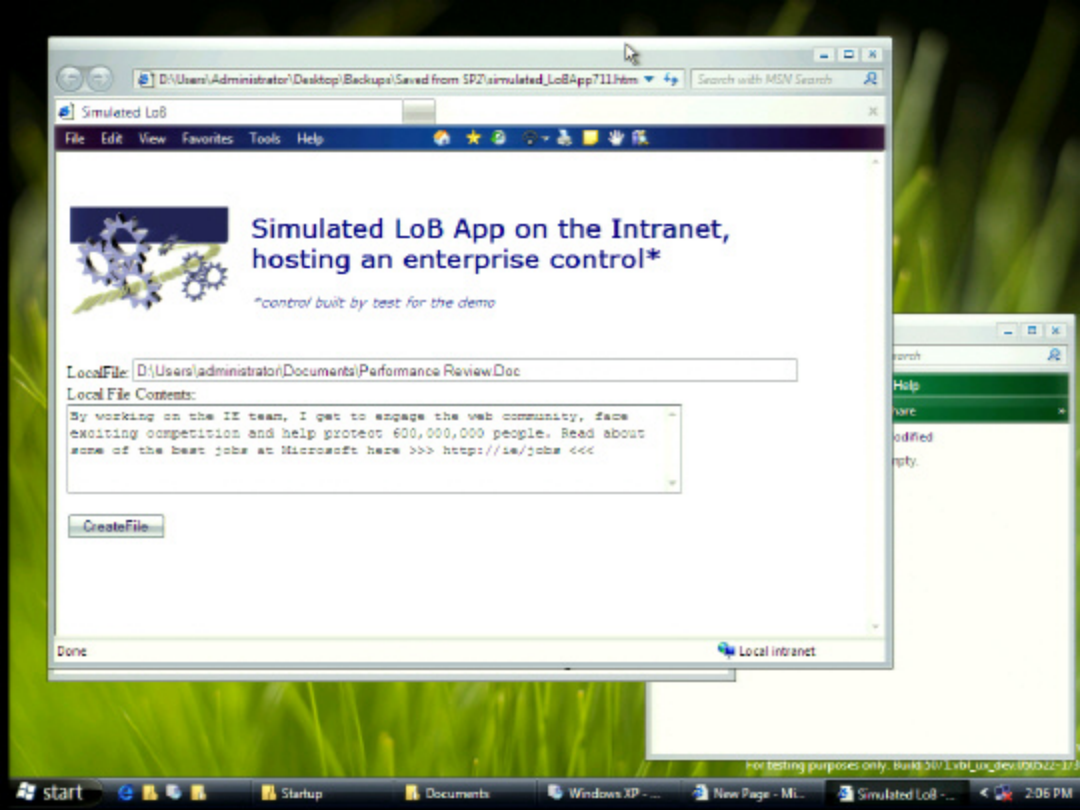

Bad Ax
File Edit View Favorites Tools Help
Home
Evil web page on the Internet, hosting a vulnerable control*
*control built by tast for the demo
LocalFile:
C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\evil.bat
Local File Contents:
FORMAT C:
CreateFile
CreateFile Failed.
Done
Internet
Startup
Search
View Favorites Tools Help
Share
Size Type Date Modified
This folder is empty.
start
Startup
Documents
Windows XP - Micr...
Bad Ax - Microsoft I...
1:52 PM

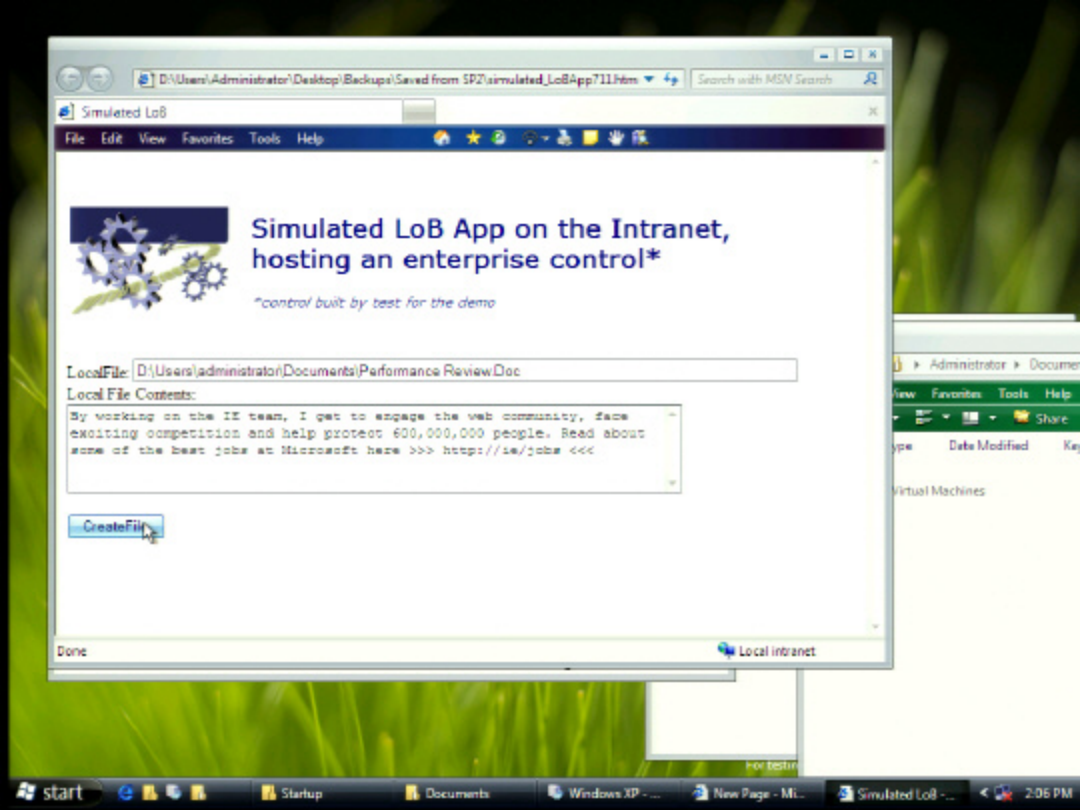
Low Rights IE on Vista

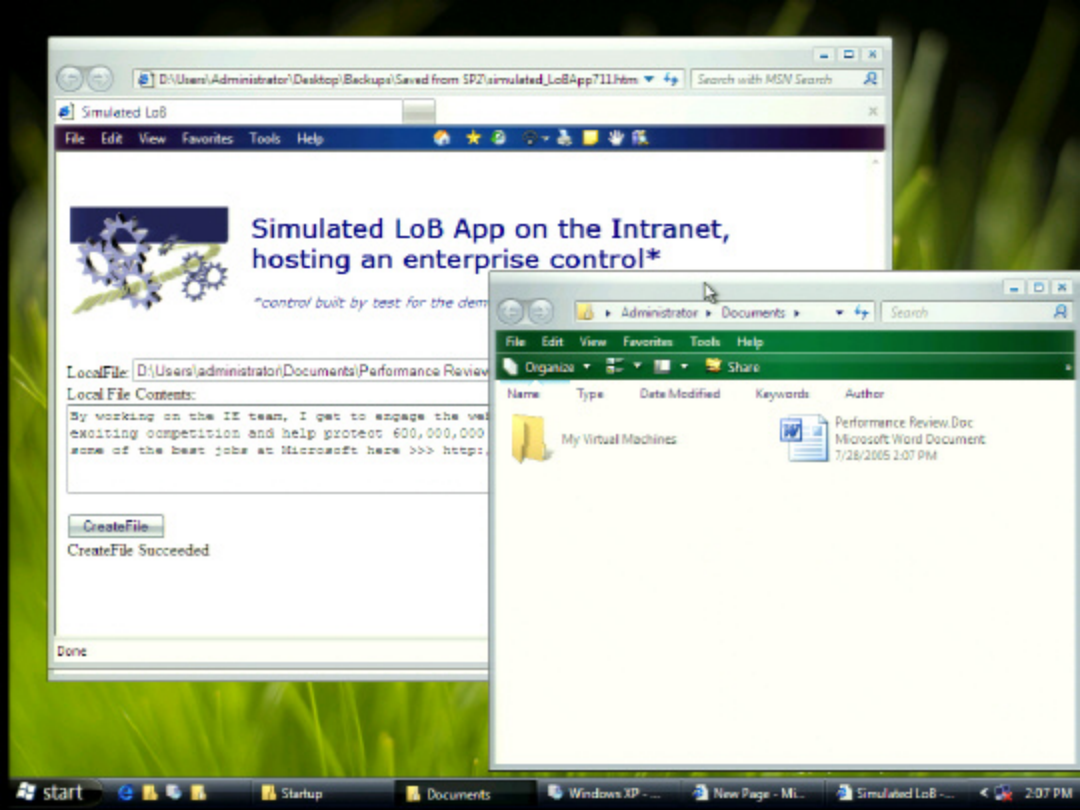


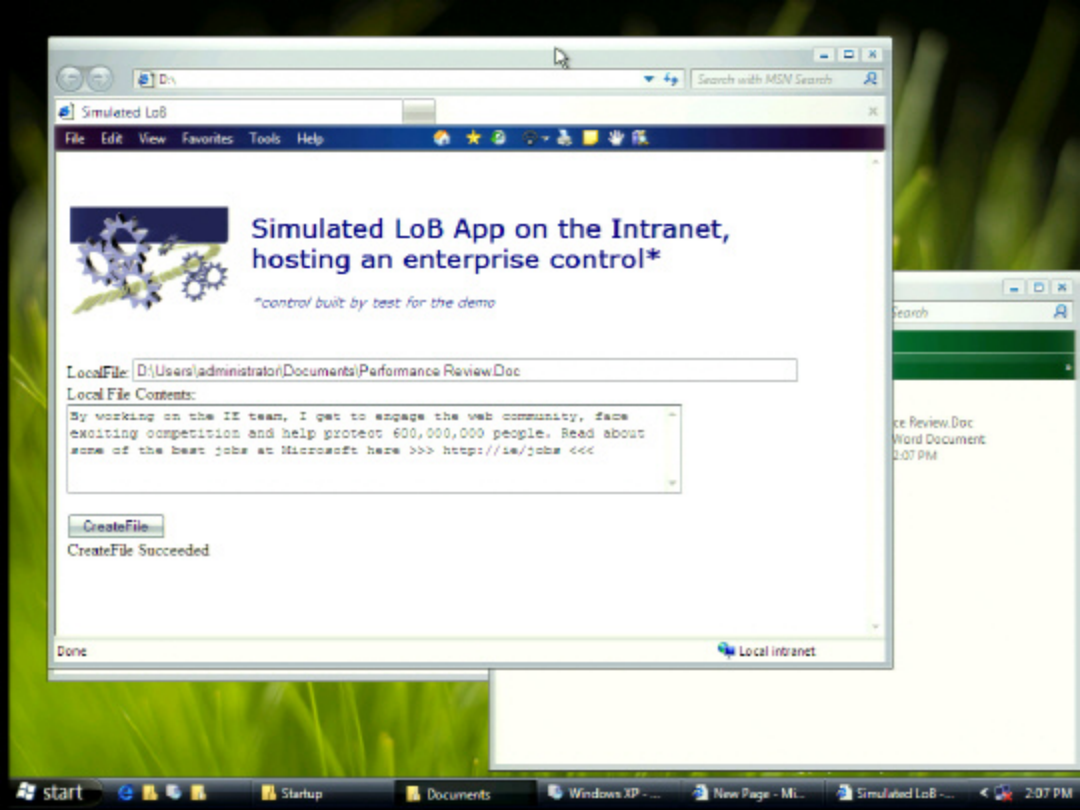

about:blank
Search with MSN Search
New Page
File Edit View Favorites Tools Help
Done
Internet
Startup
Search
View Favorites Tools Help
Share
Size Type Date Modified
This folder is empty.
start
Startup
Documents
Windows XP - Micr...
New Page - Microso...
2:05 PM


about:blank
Search with MSN Search
New Page
File Edit View Favorites Tools Help
Add to Favorites...
Organize Favorites...
6-7 Demo
Offline Backups
0 - MSN.com
1 - Evil Internet Page hosting vulnerable ActiveX Control
2 - Download the MSN toolbar
3 - Simulated LoB
1 - Evil Internet Page hosting vulnerable ActiveX Control
3 - Simulated LoB
Startup
Search
View Favorites Tools Help
Share
Size Type Date Modified
This folder is empty.
For testing purposes only. Build 5512.vbl_ux_dev.090622-1
start
Startup
Documents
Windows XP - Micr...
New Page - Microso...
2:05 PM


D:\Users\Administrator\Desktop\Backups\Saved from SPZ\simulated_LoBApp711.htm
Search with MSN Search
Simulated LoB
File Edit View Favorites Tools Help
Simulated LoB App on the Intranet, hosting an enterprise control*
*control built by test for the demo
LocalFile: D:\Users\administrator\Documents\Performance Review.Doc
Local File Contents:
By working on the IE team, I get to engage the web community, face exciting competition and help protect 600,000,000 people. Read about some of the best jobs at Microsoft here >>> http://ie/jobs <<<
CreateFile
Done
Local intranet
start
Startup
Documents
Windows XP - ...
New Page - Mi...
Simulated LoB - ...
2:06 PM


D:\Users\Administrator\Desktop\Backups\Saved from SPZ\simulated_LoBApp711.htm
Search with MSN Search
Simulated LoB
File Edit View Favorites Tools Help
Simulated LoB App on the Intranet, hosting an enterprise control*
*control built by test for the demo
LocalFile: D:\Users\administrator\Documents\Performance Review.Doc
Local File Contents:
By working on the IE team, I get to engage the web community, face exciting competition and help protect 600,000,000 people. Read about some of the best jobs at Microsoft here >>> http://ie/jobs <<<
CreateFile
Done
Local intranet
Administrator ▸ Documents
View Favorites Tools Help
Share
Type
Date Modified
Virtual Machines
start
Startup
Documents
Windows XP - ...
New Page - Mi...
Simulated LoB - ...
2:06 PM


D:\Users\Administrator\Desktop\Backups\Saved from SPZ\simulated_LoBApp711.htm
Search with MSN Search
Simulated LoB
File Edit View Favorites Tools Help
Simulated LoB App on the Intranet, hosting an enterprise control*
*control built by test for the dem
LocalFile: D:\Users\administrator\Documents\Performance Review
Local File Contents:
By working on the IE team, I get to engage the ve
exciting competition and help protect 600,000,000
some of the best jobs at Microsoft here >>> http:
CreateFile
CreateFile Succeeded
Done
Administrator ▸ Documents ▸
Search
File Edit View Favorites Tools Help
Organize
Share
Name Type Date Modified Keywords Author
My Virtual Machines
Performance Review.Doc
Microsoft Word Document
7/28/2005 2:07 PM
start
Startup
Documents
Windows XP - ...
New Page - Mi...
Simulated LoB - ...
2:07 PM


D:\
Search with MSN Search
Simulated LoB
File Edit View Favorites Tools Help
Simulated LoB App on the Intranet, hosting an enterprise control*
*control built by test for the demo
LocalFile: D:\Users\administrator\Documents\Performance Review.Doc
Local File Contents:
By working on the IE team, I get to engage the web community, face exciting competition and help protect 600,000,000 people. Read about some of the best jobs at Microsoft here >>> http://ie/jobs <<<
CreateFile
CreateFile Succeeded
Done
Local intranet
Search
ce Review.Doc
Word Document
2:07 PM
start
Startup
Documents
Windows XP - ...
New Page - Mi...
Simulated LoB -...
2:07 PM